



Euroopa Liit
Euroopa
Regionaalarengu Fond



Eesti tuleviku heaks



Eesti infoühiskonna AASTARAAMAT 2011/2012



MAJANDUS- JA
KOMMUNIKATSIOONI-
MINISTEERIUM

Eesti infoühiskonna AASTARAAMAT 2011/2012





Trükis on rahastatud ELi struktuurivahendite programmist „Infoühiskonna teadlikkuse tõstmine”. Koostanud Riigi Infosüsteemide Osakond (RISO), Majandus- ja Kommunikatsiooniministeerium.

Elektroonilised infoühiskonna aastaraamatud aadressil: www.riso.ee/et/publikatsioonid/aastaraamatud

Kujundus ja küljendamine: Eva Unt, Director Meedia OÜ
Illustratsioonid: Triinu Lille
Toimetaja: Karin Kastehein, Director Meedia OÜ
Tõlkija: A&A Lingua OÜ

ISSN 2228-3358

Sisukord

5 INFOÜHISKONNA LÜHIKRONOLOOGIA

1. peatükk AVATUD ANDMED

- 12 Avaandmed – samm tuleviku internetti, U. Vallner
- 18 Avaandmete varamu, U. Vallner, T. Tammet, A. Reitsakas
- 22 Avatud ruumiandmed, K. Teiter

2. peatükk ROHELINE IT

- 28 Roheline IKT kui keskkonnasäästu ja kulude kokkuhoiu võimaldaja, K. Kitsik
- 30 Ökoinnovatsiooni toetamine IKT lahenduste abil, K. Kitsik
- 32 Nutikas Vormsi toob saarele taastuenergia ja kaugtöökohad, I. Petersoo
- 34 E-veeseleht – metsandussektori asjaajamine paberilt elektroonseks, M. Ridala

3. peatükk KÜBERTURVALISUS

- 38 Küberjulgeolekust, H. Raud
- 40 Riigi Infosüsteemi Ameti roll Eesti küberturvalisuse tagamisel, T. Vaks
- 43 Eesti turvalisemat üleilmset küberruumi ehitamas, L. K. Ilves
- 46 Infoturbe koosvõime raamistiku ver 2, J. Tepandi
- 48 Koostöö laste turvalisema internetikasutuse edendamiseks, K. Kuusk

4. peatükk KIIRE INTERNET

- 54 Eesti kogemus lairibaühenduste arendamisel, O. Harjo
- 57 4G – Eesti mobiilse interneti võimalused ja edulugu, A. Meentalo
- 59 4G mobiilne internet maapiirkondadesse, A. Kaarekson

5. peatükk E-IDENTITEET

- 62 Kümme aastat eID ökosüsteemi, T. Martens, M. Erlich, T. Valdlo, U. Vallner
- 66 Ainulaadne mobiil-ID, H. Laasik
- 68 Digi-IDst on abi, H. Laasik
- 70 Kuidas eID ökosüsteem oma teenuse heaks tööle panna?, U. Keskel
- 72 Digitaalne tempel, A. Ljaš
- 73 Digitaalne allkiri Eestis ja Euroopas – vaade tagasi ja edasi, T. Martens

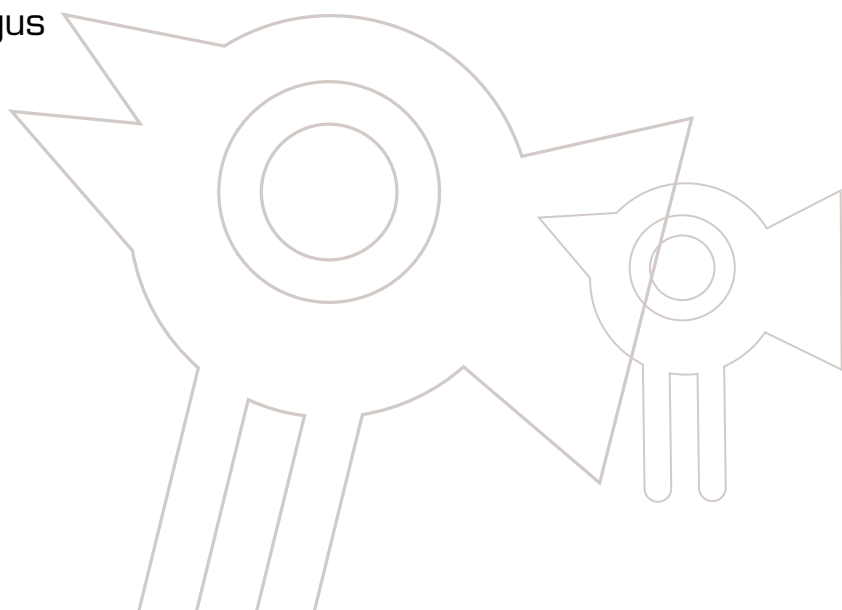
6. peatükk X-TEE

- 78 Esimesed kümme X-tee aastat, A. Kalja
- 81 Ontoloogiad ja X-tee teenuste semantiline kirjeldamine, H.-M. Haav
- 84 Andmekogude turvaline koondamine, J. Willemson
- 85 X-tee võimalikkusest teises riigis, M. Oit, A. Ansper

90 STATISTILINE ÜLEVAADE 2011–2012



aasta
andmete
elektrooniliselt e-valitsemise
teenuste välja
kõrghariduse kvaliteeti e-tervise arutletakse
maailma ID-kaart üle liidu avalik oma mobiiltelefoni
lisaks kokku kommunikatsiooniministeerium mobiil-ID ole
võimaldab konkurentsivõime hakkab kohalike
toimub Eesti e-Riik moel
arendustegevuse esitada abil
valmib demokraatia internetiga infoühiskonna saab
juhend majandus infotehnoloogia kaudu selle
konverents kohta olema esimese jälgida eestvedamisel
omavalitsuse eesmärk kaasas avalike võimalik
antud kõik kasutada info
akadeemia IKT valmib
avatud infosüsteemide
uuring
töörühm keskendub
eesmärgiks
käigus



Infoühiskonna lühikronoloogia 2011 – juuli 2012

Jaauar 2011 Majandus- ja Kommunikatsiooniministeeriumi tellimusel valmib Praxise ja e-Riigi Akadeemia uuring digi-TV ja mobiiltelefoni kasutusvõimaluste kohta avalike teenuste osutamisel. http://www.riso.ee/et/files/DigiMobi_uuring_2011_final.pdf

Veebruar 2011 Avatakse e-riigihangete veebikeskkond, mis koosneb infoportaalist ja riigihangete registrist ning võimaldab teha kõiki riigihankealaseid toiminguid elektroonselt ühes kohas. <https://riigihanked.riik.ee>

Riik hakkab väljastama mobiil-ID sertifikaate. See on alternatiiviks ID-kaardile ning võimaldab elektroonilist isikutuvastamist ja digitaalset allkirjastamist mobiiltelefoni abil. Mobiil-IDd on võimalik kasutada ka valimistel elektrooniliseks hääletamiseks. <http://www.politsei.ee/et/teenused/isikut-toendavad-dokumendid/mobiil-id>

Toimub Garage48, kus internetiteenuste arendajad loovad ühe nädalavahetuse jooksul ühiskondlikult kasulikke avalikke teenuseid. Võidab 112 Mobile – mobiili- ja veebirakendus, millega saab hädaabikõne teha ilma helistamata. <http://garage48.org/blogger/garage48-public-services-ideas-in-process>

Märts 2011 Toimuvad Riigikogu valimised. Eestlastel on viiendat korda võimalik anda oma hääl elektrooniliselt. Internetivalijate osakaal on järjest kasvanud, ulatudes seekord 24,3%ni kõigist valijatest. Esimest korda on isikutuvastuseks võimalik kasutada ka mobiil-IDd, mis muudab hääletamise eriti mugavaks, kuivõrd ei eelda ID-kaardilugeja olemasolu arvutis. <http://www.vvk.ee/valijale/e-haaletamine/e-statistika>

Arengufond loob tulevikutrendide blogi Fututuba, kus tulevikuseire eksperdid vahendavad lugejaile maailma nimekate mõttekeskuste ja uurimisasutuste mõtteavaldusi. <http://www.fututuba.ee>

Aprill 2011 Riigikantselei võtab kasutusele uue eelnõude infosüsteemi (EIS), mis võimaldab jälgida eelnõude menetlusi, leida infosüsteemis olevaid dokumente ning esitada kooskõlastamisel oleva dokumendi kohta arvamusi. Lisaks saab eelnõu koostaja EISI kaudu esitada selle avalikuks konsultatsiooniks osalusveebi <http://www.osale.ee>. <http://eelnoud.valitsus.ee/main#AU7f8ABZ>

USA inimõigusorganisatsiooni Freedom House'i uuring kuulutab Eesti maailma kõige vabama internetiga riigiks. Eestile järgnevad Ameerika Ühendriigid, Saksamaa, Austraalia ning Suurbritannia. <http://www.freedomhouse.org/report/freedom-net/freedom-net-2011>

Mai 2011 Avatakse kodanikele mõeldud ning vaba kontoritarkvara portaal LibreOffice, millel on eesti keele tugi ning mis sisaldab interaktiivset õppematerjali.
<http://www.libreoffice.ee>

Valmib Riigikogu valimiste *online*-kampaania analüüs, kus uuritakse, kui palju kasutajad erakonnad ja üksikkandidaadid interneti, sh sotsiaalvõrgustikke, oma kampaaniate korraldamiseks valimiste-eelsel perioodil.
<http://www.ega.ee/et/node/853>

Juuni 2011 Riigi Infosüsteemide Arenduskeskus (RIA) kujundatakse ümber Riigi Infosüsteemi Ametiks. Ameti uus funktsioon on järelevalve nii elutähtsate teenuste turvalisuse kui ka uute infosüsteemide loomise üle. <http://www.ria.ee>

Elektroniline majandusaruannete keskkond võidab maailma parimate e-lahenduste konkursil World Summit Award (WSA) 2011 esikoha. Aruandluskeskkond teeb andmete sisestamise ja edastamise ettevõtjatele palju mugavamaks, sest kõikide nõutud andmete esitamiseks on olemas üks kindel koht, vorm ja viis.
<https://ettevotjaportaal.rik.ee>

Juuli 2011 Keskkonnaamet avab e-teenuste portaali. Esimese elektroonse teenusena pakutakse klientidele võimalust koostada ja esitada keskkonnatasu deklaratsioone.
<https://eteenus.keskkonnaamet.ee>

August 2011 Valmis saab Eesti maapiirkondi kiire internetiga varustava lairibavõrgu EstWin esimene osa, millega on fiiberoptiliste kaablite abil ühendatud kõik Eesti linnad. Aastaks 2015 peab Eestis olema välja ehitatud fiiberoptiline baasvõrk arvestusega, et 98% majapidamistest, ettevõtetest ja asutustest paiknevad baasvõrgu liitumispunktile lähemal kui 1,5 km. Selle eesmärgi saavutamiseks peab Eesti Lairiba Arendamise Sihtasutus välja vahetama kokku üle 6000 km optilisi kaableid ning looma üle 1400 võrguühenduskoha. <http://www.elasa.ee>

September 2011 Tallinnas toimub rahvusvaheline e-valitsemise konverents ICEGOV 2011. ÜRO egiidi all toimuv suurüritus toob kokku e-valitsemisega tegelevad praktikud, ettevõtjad ning akadeemikud, et arutada e-valitsemise arenguid ning jagada kogemusi. Eesti-poolseks korraldajaks on e-Riigi Akadeemia.
<http://www.icegov.org>

Majandus- ja Kommunikatsiooniministeeriumi korraldamisel toimub iga-aastane infoühiskonna konverents, mis keskendub autoriõigustele digiajastul ning kannab pealkirja „Õigus luua, õigus tarbida“. Arutletakse digitaalse sisu kasutamisega seonduvate õiguste, kohustuste ja võimaluste üle muutunud tehnoloogiliste võimaluste maailmas. <http://infoyhiskond.eesti.ee>

Oktoober 2011 Toimub infotehnoloogia ja telekommunikatsiooni konverents „Visioonist lahendusteni 2011“. Peateemaks on avatud andmed ja konkurentsivõime – keskendutakse küsimustele, miks on vaja andmete vaba liikumist ja milles seisneb siin äri.
<http://www.visioonistlahendusteni2011.ee>

Avaliku sektori rolli ning senise kogemuse üle sotsiaalmeedias arutletakse seminaril „Avalik võim sotsiaalmeedias – kas sõber või kutsumata külaline?“. <http://www.ega.ee/et/node/896>

November 2011 Avatakse uuendatud riigiportaali eesti.ee, mille edasiarenduse peamised märksõnad on kasutusmugavus ning personaliseeritus. Lihtsam on nii info kui ka teenuste otsimine ja kasutamine, suuremat rõhku on pööratud ka info kättesaadavusele inglise ja vene keeles. <http://www.eesti.ee>

Lõpeb kolm aastat kestnud interneti- ja arvutikoolitusprojekt „Ole Kaasas!“, mille käigus on Vaata Maailma Sihtasutuse eestvedamisel antud uusi arvuti-teadmisi 100 000 eestimaalasele. Lisaks on tutvustatud targa töö korralda-mise võimalusi kodus ja kontoris ning loodud 35 „Ole Kaasas!“ arvutiklubi üle Eesti. <http://www.olekaasas.ee>

Majandus- ja Kommunikatsiooniministeeriumis alustab tööd infoühiskonna teenuste arendamise osakond, eesmärgiks parandada Eestis loodavate avalike teenuste kvaliteeti ja kasulikkust. <http://www.mkm.ee>

Detsember 2011

Üks Eesti e-riigi alustalasid, andmevahetuskiht X-tee, saab 10 aastaseks. X-tee kaudu jõuavad inimesteni turvalisel moel kõik riigi e-lahendused ja oluli-semad erasektori e-teenused. <http://www.ria.ee/x-tee>

Majandus- ja Kommunikatsiooniministeeriumi tellimusel valmib konsultatsioonifir-ma Ernst & Youngi teostatud uuring „The Role of Green ICT in Enabling Smart Growth in Estonia“. Uuringu eesmärgiks oli kaardistada roheline IKT valdkonna hetkeseis ja arengupotentsiaal Eestis. Tulemused on aluseks Eesti-Norra prog-rammi „Keskkonnasõbraliku innovatsiooni arendamine IKT abil“ välja töötamiseks. http://www.mkm.ee/public/Inno_18_GreenICT.pdf

Jaanuar 2012

Möödub 10 aastat esimese ID-kaardi väljastamisest. 2012. aasta alguse seisuga on kehtiv ID-kaart ligi 1,2 miljonil inimesel, kellest umbes 85% on Eesti kodanikud ning 15% välismaalased. Kümne aasta jooksul on kokku an-tud 72,6 miljonit digiallkirja ning vähemalt korra on dokumenti elektrooniliselt kasutanud pea pooled ID-kaardi omanikud. <http://www.id.ee>

Eesti IKT-ettevõtteid koondav Demokeskus saab kolmeaastaseks. Keskus ra-jati selleks, et suurendada Eesti kui e-riigi nähtavust rahvusvahelisel areenil ning hoogustada kohalike IKT-teenuste ja -kogemuste ekspordi. <http://e-estonia.com>

Eesti teeb maailmarekordi e-rahvaloenduse osalejate osakaaluga, lüües se-nist Kanada 54%st tulemust 8 protsendipunktiga (62%). <http://www.stat.ee/rel2011>

Veebruar 2012

Eestis hoogustub avalik arutelu infoajastu autoriõiguse ning ACTA lepingu üle. Debati käigus töötatakse välja Eesti internetivabaduse teesid. Mõttepaberi eesmärgiks on algatada ühiskondlik diskussioon internetikasutajate põhiõigus-te teemal. http://mottehommik.praxis.ee/uued_teesid

Eesti Infotehnoloogia Sihtasutus (EITSA) hakkab ellu viima info- ja kommuni-katsioonitehnoloogia kõrghariduse ning teadus- ja arendustegevuse riiklikku programmi. Eesmärk on tõsta Eesti IKT kõrghariduse kvaliteeti ja rahvusvahe-list konkurentsivõimet ning valdkonna teadus- ja arendustegevuse võimekust. <http://www.eitsa.ee>

Märts 2012

Infotehnoloogia ja Telekommunikatsiooni Liidu eestvedamisel toimub IT öö, mille raames mõtleavad sajad noored üle Eesti välja ideid, kuidas IT kaudu elu koolis põnevamaks muuta. Üritus on osa IT-erialade populariseerimise projek-tist „Kõik on IT“. <http://startit.ee/it-oo-2012-valminud-tood>

14. märtsil täitub Eesti ID-kaardil 500 000 unikaalset elektroonilist kasutajat.

Aprill 2012

Eesti ühineb avatud valitsemise partnerlusega (Open Government Partner-ship), mille eesmärk on toetada demokraatiat, majandusarengut ning koos-

tööd valitsusväliste organisatsioonidega.
<http://www.opengovpartnership.org>

Avatakse Tallinna vanalinna 3D-mudel, mis annab võimaluse tutvuda nii pealinna kultuuriväärtuslike ehitiste kui ka toitlustus- ja ööbimiskohtadega uudsel moel.
<http://3d.tallinn.ee>

Mai 2012 Toimub e-demokraatia konverents „Demokraatia muutuste keerises“. Konverentsil arutatakse muuhulgas, milline peab olema põhiseaduslik demokraatia infoühiskonnas ning millisena näevad kodanikud oma rolli demokraatlikus riigikorralduses.
<http://infoyhiskond.eesti.ee>

Valitsus moodustab infoühiskonna nõukogu, mis asendab 1996. aastast tegutsenud informaatikanõukogu ja kaasajastab selle ülesandeid ning koosseisu. Nõukogu ülesandeks on seisukohtade esitamine ja valitsuse nõustamine infoühiskonna arengut puudutavates olulistest küsimustes.

President Toomas Hendrik Ilves, Euroopa Liidu e-tervise töörühma juht, teeb ülevaate e-tervise töörühma aruandest „Tervishoiu ümberkorraldamine Euroopas aastaks 2020“. Eesti riigipea juhitud töörühma kuulusid eri riikide tervishoiueksperdid, patsientide, meditsiini-, ravimi- ja IKT-tööstuse esindajad, õiguseksperdid ja poliitikud.

<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/453&age=d=O&language=EN&format=HTML&guiLanguage=en>

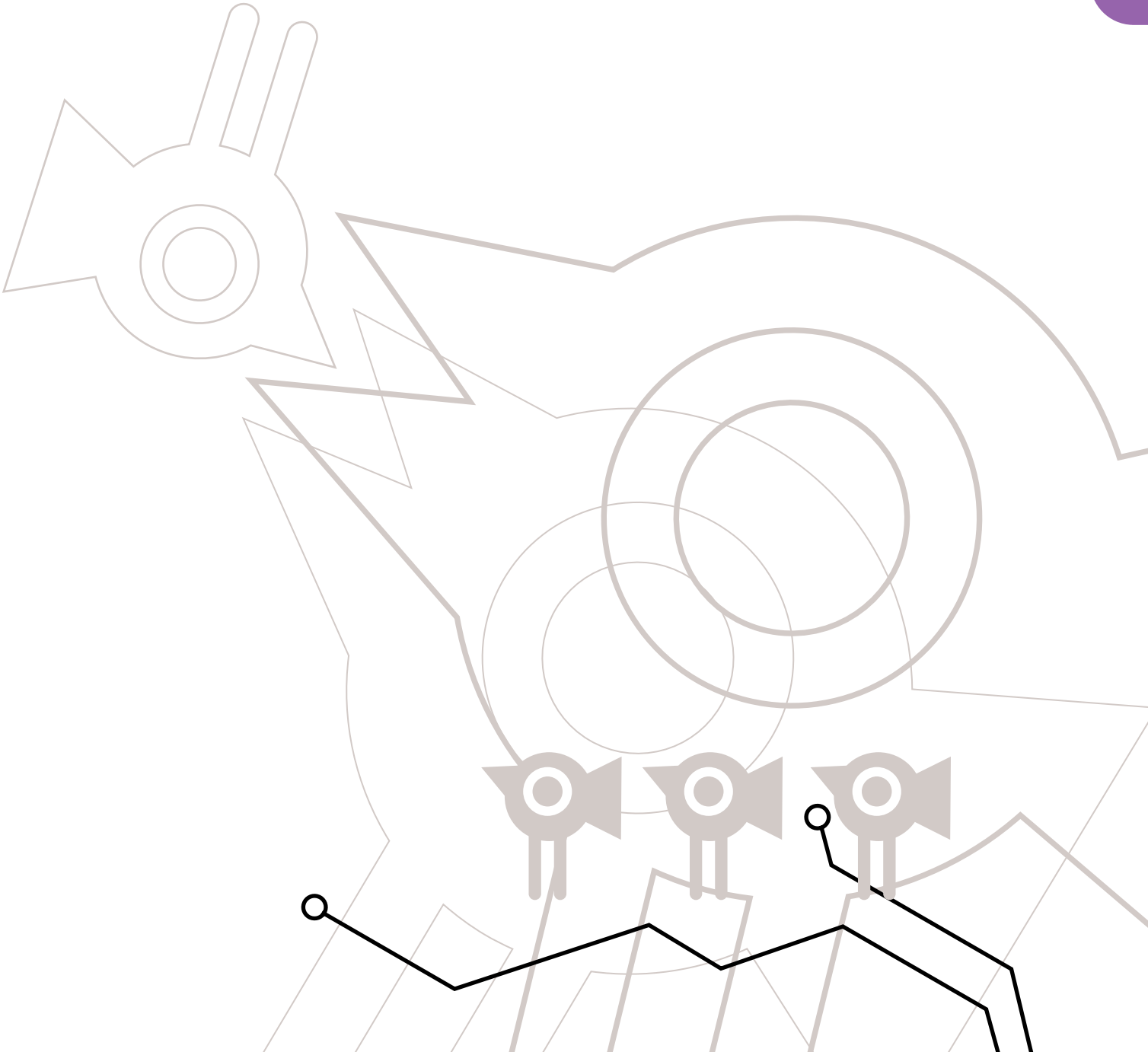
Juuni 2012 Konkursi „Eesti parim m-teenus 2012“ üldvõitjaks ning meelelahutuse ja meedia kategooria võitjaks kuulutatakse Eesti Rahvusringhäälingu mobiilirakendus ERR, millega saab jälgida ERRi kõigi tele- ja raadioprogrammide otseülekandeid ning saadete arhiivi. <http://www.m-konkurss.net>

e-Riigi Akadeemial valmib programmi „Infoühiskonna teadlikkuse tõstmine“ raames juhend kohalike omavalitsuste veebisuhtluse arendamiseks. Juhend keskendub eelkõige olemasolevate tehniliste lahenduste kasutamise tõhustamisele, käsitledes nii kohalike omavalitsuste teenusportaali kui ka sotsiaalmeedia platvormide kasutamist.

<http://www.ega.ee/files/Soovitused%20kohalike%20omavalitsuste%20veebisuhtluse%20interaktiivsuse%20t%C3%B5stmiseks.pdf>

Juuli 2012 Avaneb taotlusvoor avaliku teabe taaskasutatavaks muutmisele suunatud projektide finantseerimiseks. Toetatakse infosüsteemide muutmist nii, et teave oleks masinloetaval kujul kättesaadav avaandmete portaalis opendata.riik.ee.
<http://www.ria.ee/36610>

Konsultatsiooniringile läheb infoühiskonna arengukava 2020 koostamise ettepanek. Eesmärk on leppida partnerluses era- ja kolmanda sektoriga kokku, kuidas kasutada IKTd parimal moel Eesti konkurentsivõime tõstmiseks ja inimeste heaolu parandamiseks. <http://infoyhiskond.eesti.ee>







1. PEATÜKK

AVATUD ANDMED

Avatud andmete ehk avaandmete teemast ei saa tänapäeval mööda vaadata enam ükski riik. Sellest on saanud meie igapäevaelu osa – juba praegu toodavad, koguvad ja säilitavad avaliku sektori asutused mitmesuguseid andmeid digitaalsel kujul, olles ahvatlevaks toormaterjaliks kõikvõimalikele uutele teenustele ja toodetele. Avaandmete all mõistetakse kõigile vabalt ja avalikult kasutamiseks antud masinloetavas formaadis andmeid, millel puuduvad kasutamist ning levitamist takistavad piirangud. Ka Eesti avaliku teabe seadus kohustab avaliku sektori juurdepääsupiiranguta infot avalikustama (kas veebisaidi, dokumendiregistri või andmekogu kaudu). See peatükk annab ülevaate avaandmete teemast ja põhimõtetest nii Eestis kui ka välismaal.



Avaandmed – samm tuleviku internetti



UUNO VALLNER

uuno.vallner@riso.ee

Majandus- ja Kommunikatsiooniministeerium

Viiekümneandel sõnastatud avaandmete (*open data*) ja avatud riigi (*open government*) põhimõte muutus uue sajandi alguseks lööksõnaks. Nüüd on see aga muutunud kogu ühiskonda mõjutavaks tegevussuunaks. Avaandmed on esimene etapp liikumises n-ö asjade interneti ja lingitud maailma poole. Just andmete linkimises nähakse võimalust, kuidas suuremahulise infohulgaga (*big data*) tulevikus toime tulla.

Meilgi võiks üheks eesmärgiks olla „lingitud Eesti“ – eestimeelne IKT toel loodud hajutatud isikute, organisatsioonide, tarkade seadmete, teadmiste, infosüsteemide, linkandmete koosvõimeline võrgustik. Selle loomine eeldaks läbimurret sellistes suundades nagu ülikiire andmesidevõrk ja targad seadmed, koosvõimelised infosüsteemid, teadmusvõrgustikud, semantilised võrgustikud, linkandmed ja avatud riigi tehnoloogiad (avatud standardid ja andmed, vaba tarkvara).

Taaskasutuseks avatud andmed

Avaliku sektori asutused toodavad, koguvad või säilitavad suurt hulka teavet ja infosisu, nagu statistika, ruumiandmed, majandusandmed, keskkonnaandmed, arhiivimaterjalid, raamatud, kunstikogud. Tänapäeval on need ressursid väga suurel määral digitaalsel kujul ja kujutavad endast suurt väärtust uute toodete või teenuste juures, kus kasutatakse neid andmeid toormaterjalina. Erilist taaskasutamise huvi pakuvad dünaamiliselt muutuvad andmed avaliku sektori registrites.

Euroopa Liidu tellitud uuringu¹ kohaselt on ELi 27 riigis avaliku sektori teabe suurema avatu-

se ja hõlpsa juurdepääsu võimaldamise kaudu võimalik saavutada majanduslikku kasu ligikaudu 40 miljardit eurot aastas. Taaskasutuse turg Euroopas kasvab aastas 7–40%. Euroopa Komisjoni asepresident Neelie Kroes on nimetanud avatud andmeid lausa uueks kullaks²: „Kui naftat nimetada mustaks kullaks, siis andmete taaskasutamine oleks Euroopale uus kuld“. Avaliku sektori andmete avamine võimaldab erasektoril kombineerida neid teiste andmetega ja luua uusi lisaväärtusega äriteenuseid. Avalik sektor saaks keskenduda oma põhitegevusele ja loobuda konkureerimisest erasektoriga. Kuid andmete esitamine taaskasutataval kujul toob kaasa kulutusi. Euroopa Komisjoni uuringu alusel võimaldaks 1,4 miljardi suurune avaliku sektori poolne investeering suurendada Euroopa SKP käivet 140 miljardi euron. Seega iga investeeritud sent suurendaks riigi SKPd euro võrra.

Avatud andmed on taaskasutatavad kullapada

Andmete taaskasutamise teema pole uus. Sellest hakati rääkima juba 50. aastate lõpus. Nõukogude ajal taaskasutas näiteks tollane informatsiooni instituut referaatide välisbaase magnetlihtidel kogumahuga üle miljoni kirje aastas³. Taasiseseisvunud Eesti esimeseks registri taaskasutamise juhiks oli 1995/96 loodud Riigi Teataja tehnoloogiline lahendus. Selle väljaandmiseks paberikujul kasutati WordPerfecti kontoritarkvara. WordPerfecti failid konverteeriti SGMLi (xml on SGMLi derivaat) vormingusse, signeeriti digitaalselt ja avati ftp serveri kaudu kõigile vabaks kasutamiseks. Õigusaktide aktiivsemad taaskasutajad

olid Riigikantselei dokumendihaldussüsteem, Riigi Teataja *online*-andmebaas, IBSi otsisüsteem ja EstLex. Viimastel aastatel on paljud riigid avastanud, et andmete avamisega on võimalik elavdada majandust, ja alustanud ulatuslikke andmete taaskasutamist toetavaid projekte:

- Euroopa Komisjoni avaandmete poliitika⁴,
- Komisjoni tellitud uurimus „Towards a pan EU data portal – data.gov.eu“⁵,
- Suurbritannia avatud andmete põhimõtted⁶,
- W3C avatud andmete põhimõtted⁷,
- Open Government Data avatud andmete arendamisgrupi soovitus⁸,
- USA ja UK soovitus OECD-le avaandmete poliitika osas⁹,
- OFKN Open Data käsiraamat (juriidika, sotsiaalia, tehnoloogia).

Paljud riigid, regioonid ja omavalitsused on taaskasutuseks loonud raamistikud ja taaskasutat lihtsustavad portaalid.

- Euroopa avaandmete koondkataloog
<http://publicdata.eu>
- USA avaandmete kataloog
<http://data.gov>
- UK avaandmete kataloog
<http://data.gov.uk>
- Austraalia avaandmete kataloog
<http://data.gov.au>
- Kanada avaandmete kataloog
<http://data.gc.ca>
- Keenia avaandmete kataloog
<http://opendata.go.ke>
- Norra avaandmete kataloog
<http://data.norge.no>
- Hollandi avaandmete kataloog
<http://data.overheid.nl>
- Uus-Meremaa avaandmete kataloog
<http://data.govt.nz>
- Itaalia avaandmete kataloog
<http://data.gov.it>
- Prantsusmaa avaandmete kataloog
<http://data.gouv.fr>
- Rootsi avaandmete kataloog (eraisiku initsiaatiivina)
<http://www.opengov.se>
- Philadelphia piirkonna avaandmete kataloog
<http://opendataphilly.org>
- Helsingi piirkonna omavalitsuste avaandmed
<http://www.hri.fi/en>
- CKAN avaandmete kataloog/hoidla
<http://thedatahub.org>

Kuigi andmete avamine taaskasutuseks toob kaasa tuntava kulu, on poliitikud tunnetanud selle tu-

gevat mõju riigi majandusele ja asunud aktiivselt investeerima avaandmete infrastruktuuri loomisse ja arendamisse. USA president Obama kirjutas oma esimesel valitsemispäeval alla avatud ja läbipaistva riigi memorandumile, mille kohaselt avalik sektor avas oma andmed taaskasutuseks. Juba 2011. aasta sügiseks sisaldas USA avaandmete kataloog 390 000 andmehulka.

Mis on avaandmed?

Avaandmed ja andmehulgad. Taaskasutuseks publitseeritud andmeid nimetatakse avatud andmeteks (*open data*) ehk avaandmeteks. Selle all mõistame kõigile avalikult vabalt kasutamiseks antud, veebisaitidest kättesaadavaid, masinloetavas vormingus andmeid ilma kasutamise-, patente- ja levitamispiranguteta. Kui seaduses ei ole andmete hankimise eest ette nähtud tasu, saab avaandmeid kätte tasuta ja ilma ligipääsu kitsendusteta.

Avaliku teabe seadus¹⁰ kohustab avalikustama avaliku sektori juurdepääsupiranguteta info asu-

Taaskasutamiseks sobivad vabavaraliste rakendustega avatavad ja töödeldavad vormingud.

tuse veebisaidi, dokumendiregistri ja andmekogude kaudu. Lisaks lasub avalikul sektoril kohustus väljastada teavet vastavalt esitatud teabenõuetele. Siin räägime avaandmetest kui infost, mis esitatakse avalikkusele proaktiivselt avatud vormingutes. Avaandmete allalaadimise jaoks ei ole üldjuhul vaja teabenõuet esitada.

Ametkondlikult loodud andmete avalikustamisel on mitu olulist eesmärki, kõige konkreetsem neist on isikute, ettevõtete ja kolmanda sektori huvi kas lihtsalt tutvuda olemasolevate andmetega või kasutada neid oma tarkvararakendustes lisaväärtuse loomiseks mingis valdkonnas.

Avalikustamisele kuuluvad kõik nii riigiametite kui ka kohalike omavalitsuste loodud andmed, mille avalik kasutus ei ole otseselt keelatud ning mis sisaldavad ka muid andmeid peale isikuandmete. Andmetest, mis sisaldavad nii isikuandmeid kui ka muid andmeid, avalikustatakse ainult viimased.

Avaandmete kontekstis nimetame terviku moodustavaid andmeid andmehulgaks (*dataset*). »»

» Need võivad olla näiteks lepingutekstitid, määruste tekstid, kirjavahetuse metainfo kogud, eelarve- ja statistikafailid, avatud vormingusse konverteeritud andmebaasid/registrid või registritest andmeid väljastavad avatud võrguteenused. Üksikuid lepinguid, määrusi jne ei ole mõistlik käsitleda eraldi andmehulgana, erinevalt üksikust andmebaasist. Mõne andmehulga puhul piisab kasutajale teabele juurdepääsust (lugemiseks, kopeerimiseks), mõne puhul on olemas tugev taaskasutamise huvi. Allpool on valdkonnad järjestatud (vastavalt OECD 2006. aasta analüüsile) taaskasutamiseväärtuse kasvavas järjekorras:

- kultuur (raamatukogud, arhiivid, muuseumid, ringhääling),
- poliitika (pressiteated, strateegiad, rohelised raamatud),
- haridus (loengud, õppematerjalid),
- teadus (ülikoolide, instituutide ja avaliku sektori uuringud),
- õigusinfo (kohus, õigusaktid, patendid, kaubamärgid, õigused ja kohustused),
- loodus (bioloogiline, ökoloogiline, geoloogiline ja geofüüsikaline info, teave energiaressurssidest),
- põllumajandus, mets, kalandus,
- turism, majutus ja meelelahutus,
- liiklus, transport,
- sotsiaalne info (statistika, demograafia, tervis, haridus),
- majandus ja äri,
- meteoroloogia, keskkonnainfo,
- ruumiandmed.

Avalikustatav andmehulk võib tehnilises mõttes olla nii kogumik inimloetavaid tekstifailide (näiteks seaduste või määruste, ametlike teadete või lepingute kogu) kui ka masinloetavaid andmeid (näiteks csv- või xml-vormingus failideks eksportitud andmebaas või veebiteenus, mis võimaldab otsida ja alla laadida kõiki andmeid näiteks json- või xml-vormingus).

Andmehulk on tehnilises mõttes inimloetavate tekstifailide kogumik

Kasutaja peab saama:

- sirvida ja otsida avalike andmehulkade seast endale huvipakkuvat kogu;
- laadida leitud andmehulk tervikuna või teenuste pakutud otsisüsteemi kaudu osadena kohe alla, ilma et ta peaks selleks läbirääkimisi pidama või paroole hankima. Erandina võib andmehulga laadimine olla tasuline;
- kasutada andmekogu edaspidi vabalt, õigusega see tervikuna enda arvutisse laadida ja ka-

sutada oma rakendustes (nii tasuta kui ka tasulistes), ilma et ta peaks selle eest (täiendavalt) maksma või et tal oleks selleks vaja luba.

Kusjuures andmehulka looval ja avalikustaval avaliku sektori asutusel pole kohustust pakkuda andmete kasutajatele lisamugavusi, näiteks talle sobivasse vormingusse konverteerimist, spetsiaalsete võrguteenuste ehitamist, tõlkimist vms. Samuti ei ole ametkonnal kohustust tagada andmete korrektsust ega ajakohasust. Selle asemel peab avalikustaja selgitama lühidalt andmete olemust ja panema kirja nende oodatava ajakohastamise sageduse.

Andmehulga litsents ja tasu. Avaandmete hulgal peab olema litsents, mis võimaldab seda vabalt ja piiranguteta kasutada, töödelda ja levitada, kusjuures kasutaja valikul nii tasuta kui ka tasu eest. Konkreetset soovitamist litsentsiks valida *creative commons*'i litsentsi¹¹. Seal loetletud litsentsidest soovitamist eeskätt CC by 3.0 litsentsi¹². See tähendab, et oma teost litsentsides on litsentsiandjaks autor või autoriõiguste omaja, litsentsisaajaks aga üldsus. Teil on õigus teost kopeerida (reprodutseerida), levitada, esitada ja üldsusele suunata ning teha sellest kohandusi (adaptsioone), arranžeringuid ja teisi töötusi, sh tuletatud teoseid tingimusel, et viitate autorile.

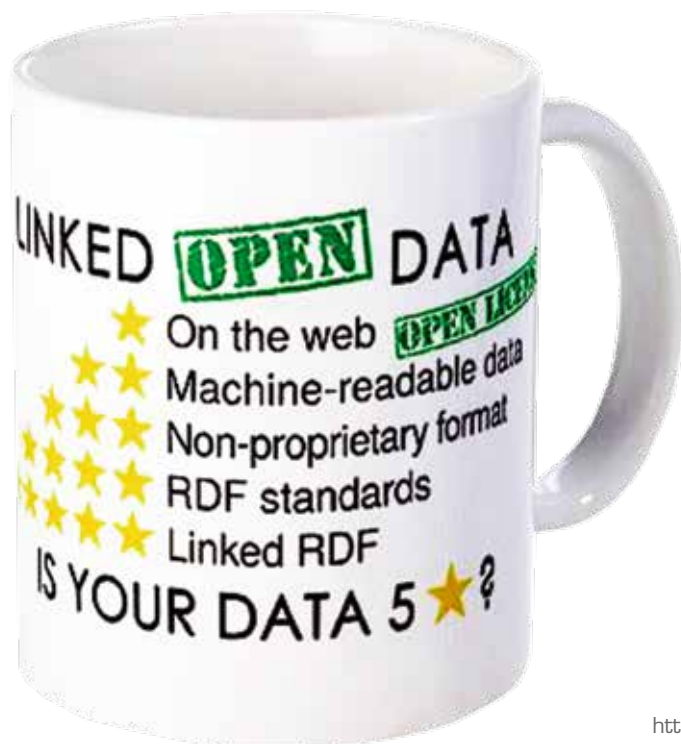
Avaandmed avalikustatakse soovituslikult tasuta allalaadimiseks, kuid selleks seadusega ettenähtud juhtudel on avalikustajal õigus nõuda andmete laadimise eest tasu.

Andmehulga avalikustamise põhimõtted. Andmehulga avalikustamise juures tuleb otsida kompromissi kahe eesmärgi vahel:

- andmete mugav kasutatavus ja arusaadavus andmete otsijale ja allalaadijale,
- andmete avalikustamise lihtsus ja avalikustaja töökoormuse minimeerimine.

Selleks tuleb esimese asjana leida kõige lihtsam, odavam ja kiirem viis olemasolevaid andmeid sellisena avalikustada ja alles seejärel uurida viise, kuidas luua mugavusi nii otsijale kui ka allalaadijale. Teisisõnu, andmete täiustamine, konverteerimine jms tööd tuleb ette võtta alles siis, kui andmehulk on juba esialgsel kujul avalikustatud.

Andmeid võib täiustada ja konvertida ka kolmas osapool, kes omakorda saab neid andmeid kas tasuta või tasu eest edasi jagada. Avatud andmehulk vastab järgmistele nõuetele¹³.



Tim Berners-Lee formaaditasemete soovitus kruusil
http://www.cafepress.com/w3c_shop

1. **Terviklus.** Kõik avalikud andmed tehakse kättesaadavaks. Selle alla loetakse kõik andmed, millele ei kehti isikuandmete jm piirangud.
2. **Pärit algallikast.** Andmed on töötluseta kogutud algallikast, säilitades oma originaalkuju ja detailsuse. Nagu andmekogudegi puhul, pole lubatud andmete võtmine teisest andmekogust.
3. **Ajakohasus.** Andmehulk on avaldatud võimalikult kiirelt, et säilitada selle asjakohasus.
4. **Kättesaadavus.** Andmed on saadavad võimalikult laiale kasutajateringile võimalikult laia kasutuseesmärgiga.
5. **Masinloetavus.** Andmed on mõistetava struktuuriga ja automaatselt töödeldavad.
6. **Diskrimineerimise vältimine.** Andmed on esitatud avalikult, kättesaamiseks pole vaja registreeruda ega taotleda juurdepääsu.
7. **Avatud standardite kasutamine.** Andmed on esitatud avatud vormingus, mis ei ole ühegi ettevõtte ega isiku ainuomand.
8. **Vaba litsents.** Andmed ei ole kaitstud autoriõiguse, patendi, kaubamärgi ega ärisaladuse seadustega. Mõistlikud privaatsus- ja turvalisuspiirangud on lubatud.

Kuidas avalikustada?

Mis vormingus? Peamise põhimõttena arvestame, et palju parem on avaldada andmed ebamugavas kodeeringus, kui jätta need esialgu avalda-

mata põhjusel, et millalgi on plaanis võtta ette kodeeringu täiustamine. Teiseks, avaldatud andmehulka saab edaspidi avaldada uues, paremas kodeeringus.

Soovitame lähtuda vormingute ja kodeeringute kasutajasõbralikkuse hindamisel Tim Berners-Lee viie täрни süsteemist¹⁴, kus suurem täрни arv tähendab kasutajale paremat vormingut/kodeeringut. Eesti oludes võiks vormingute jaotus olla järgmine:

- * andmed on veebist kättesaadavad mis tahes vormingus (nt .jpeg, .pdf, .doc, .docx, .xls). Andmeid pole võimalik failist eraldada või on esitatud omanduslikele tarkvaradele orienteeritud vormingutes;
- ** andmed on veebisaidil avatud vormingus (nt .txt, html, .odt), kuid struktureerimata kujul;
- *** andmed on veebisaidil esitatud avatud ja vabas struktuurset esitust tagavas vormingus (nt .csv, .xml, .ods);
- **** andmetes olevaid objekte identifitseeritakse URIdega¹⁵;
- ***** andmed on URIde abil lingitud teiste andmetega.

Andmehulga avaldamiseks sobivad eeskätt vormingud, mida on võimalik avada ja töödelda vabavaliste rakendustega. Selliselt on töödeldavad näiteks odt-vormingus dokumendifailid, samuti struktuursete andmete levinuimad vormingud .csv, .json, .xml.



» Olukord Eestis

Eestiski on tekkinud arvestatav poliitiline tahe muuta avaliku sektori teave enam taaskasutatavaks. Nii on valitsusprogrammi¹⁶ jaotises „E-riigist l-riigiks“ alalõik „Riigi e-varade andmine kodanike ja ettevõtete teenistusse“ pühendatud avaandmetele. Valitsusprogramm lubab sõnaselgelt:

- teeme riigi ruumiandmed töödeldaval kujul avalikuks – see annab kodanikele ja ettevõtetele võimaluse ise luua riigi andmete põhjal otstarbekaid teenuseid;
- läbipaistvuse ja kaasatuse suurendamiseks ning erasektori ergutamiseks uute rakenduste loomisele muudame avalikud ehk riigi ja kohalike omaavalitsuste andmed masinloetavaks (*machine-readable public data*);
- seame sihiks, et era- ja avaliku sektori koostöös loodud andmekogud oleksid ettevõtetele ja eraisikutele arendamiseks kättesaadavad.

Eestis tegutseb avatud andmete kogukond¹⁷, kogukonnal on lehekülg ka Facebookis. Teenuste valmistamisel on aktiivne liikumine Garage48, kelle deviisiks on „vähem juttu, rohkem tegusid“. Arvestatav on ka ITLi initsiatiiv, kelle 2011. aasta konverents „Visioonist lahenduseni 2011“ keskendus takistusele uute e-teenuste loomisel.

Eestis võib hinnata avaliku teabe kättesaadavust eeskujulikuks. Kuna üsnagi liberaalne avaliku teabe seadus¹⁸ kohustab teabevaldajaid avalikustama juurdepääsupiiranguteta info asutuse veebisaidi, dokumendiregistri ja andmekogude kaudu, siis kuulub meil avalikustamisele tunduvalt rohkem teavet kui enamikes riikides. Näiteks peab iga avaliku sektori asutus avalikustama asutuse koosseisu, palgaandmed, dokumendiregistrid, aruanded, statistika, eelarved, arengukavad. Avaliku teabe seadus eristab 32 liiki avalikustatavat teavet. Arvestades, et Eestis on 2000 avaliku sektori asutust ja iga asutus peaks avalikustama keskmiselt 10 andmehulka, on taaskasutatava teabe maht vähemalt 20 000 andmehulka.

Kuid erinevalt enamikust riikidest ei lasu avalikul sektoril kohustust avalikustada infot taaskasutataval kujul. Avalikustatud andmehulgad pole alati avatud vormingutes. Kasutatakse põhiliselt PDFi ja omanduslikule tarkvarale MS Office orienteeritud vorminguid. Seega on valdavalt tegemist ühe täрни andmetega.

Avaliku sektori info on talletatud andmebaasidesse. Kuid avalikud andmebaasid ja nende ava-

tud teenuste liidesed on kirjeldamata ja seega raskesti taaskasutatavad. Seadus ei kohusta avalikustama selliste registrite kirjeldusi ja nende teenuseid riigi infosüsteemi haldussüsteemis RIHA. Näiteks on Riigikantselei dokumendiregister eeskujulikult realiseeritud, selle väljundiks on xml-kujul andmed, kuid andmed ja otsirakenduse liides, samuti tulemuste salvestamise võimalus xml-vormingusse pole potentsiaalsetele kasutajatele kirjeldatud. Esitades dokumendiregistrile päringu kujul <https://dhs.riigikantselei.ee/avalikteave.nsf/contractsbydate?open&path=2011/12> Detsember, saame vastuse kujul:

```
<document noteid="NTOO17AE7E">
<field name="date">30.12.2011</field>
<field name="docid">L11165</field>
<field name="subject">Trükiste kujundamine ja trükkimine</field>
<field name="documenttype">Töövõtuleping</field>
<fieldname="contractstartdate">30.12.2011</field>
<field name="contractenddate">20.01.2012</field></document>
```

Kuid Riigikantselei dokumendiregister on pigem positiivne erand. Enamik taolisi registreid väljastab tulemusena HTML-teksti, mida ei saa vahetult taaskasutuseks töödelda.

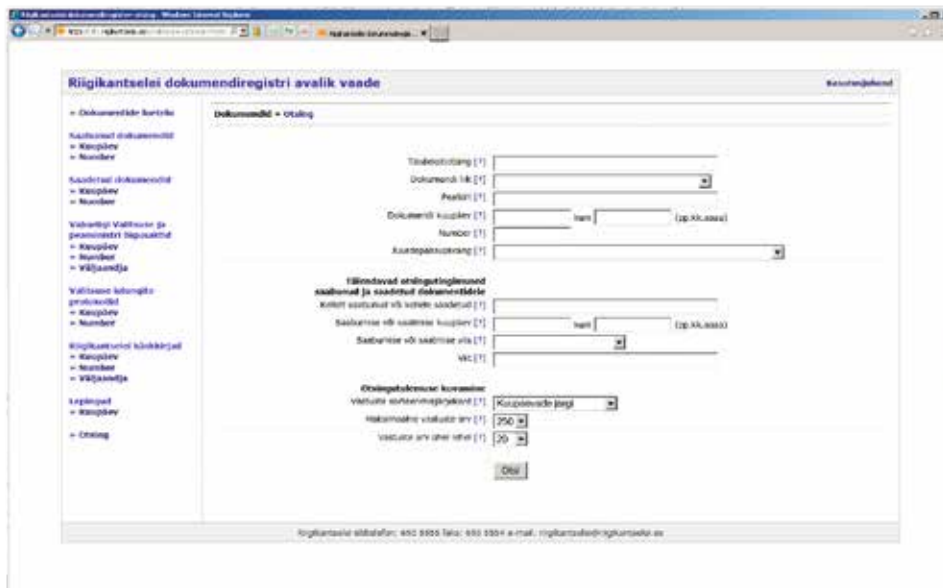
Avalikud teenused ei kaota mahalaadimise vajadust. Enamasti puudub Eesti avalikel teenustel otsitulemuste mahalaadimise võimalus, rääkimata nende vahetust *mashup*-võimalusest teiste teenustega.

Vastavalt avaliku teabe seadusele peavad andmekogus töödeldavad andmed olema avalikult kättesaadavad, kui neile ei ole seadusega või selle alusel kehtestatud juurdepääsupiirangut. Kuid andmekogus ei avalikustata isikuandmeid, kui avaldamise kohustus ei tulene seadusest. Seega peaksid olema ilma isikuandmeteta avalikud kiiruskaamerate andmed, politsei registreeritud intsidendid jms. Eesti avalik sektor on valdavalt eiranud seda nõuet ja jätnud isikuandmeid sisaldava registrite avaliku osa avalikustamata, rääkimata nende esitamisest taaskasutataval kujul.

Isikuandmeid sisaldavate registrite avalike andmete taaskasutamise võimalused on tagasihoidlikud.

Eesti avaandmed on hajutatud asutustesse. Olu- lisemad avaandmete tootjad:

- Maa-amet – geoportaal:
<http://geoportaal.maaamet.ee>



Näide päringust Riigikantselei dokumendiregistrisse

- Keskkonnateabe Infokeskus: <http://www.keskkonnainfo.ee>
- Statistikaamet: <http://pub.stat.ee/px-web.2001/dialog/statfile2.asp>
- Rahvusraamatukogu rahvusteavikute digitaalarhiiv DIGAR: <http://digar.nlib.ee>
- Rahvusarhiivi digiarhiiv

Üheks teeks avaandmete kättesaadavuse hõlbustamiseks ja avaandmete esituse korrastamiseks oleks praegu pilootrakendusena toimiv avaandmete varamu <http://opendata.riik.ee>.



- <http://epsiplatform.eu/content/review-recent-psi-re-use-studies-published>
- Neelie Kroesi kõne "Data is the new gold" 12. 12. 2011: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/872&format=HTML&age=d=0&language=EN&guiLanguage=en>
- Uno Vallner. Retrospektiivsed otsisüsteemid. Tallinn, Eesti Informatsiooni Instituut, 1985.
- http://ec.europa.eu/information_society/policy/psi/index_en.htm
- http://ec.europa.eu/information_society/policy/psi/docs/pdfs/towards_an_eu_psi_portals_v4_final.pdf
- <http://data.gov.uk/opendataconsultation>
- <http://www.w3.org/TR/gov-data>
- <http://www.opengovdata.org>
- <https://usoecd.cms.getusinfo.com/data.html>
- <https://www.riigiteataja.ee/akt/122032011010?leiaKehtiv>
- <http://creativecommons.org>
- <http://creativecommons.org/licenses/by/3.0>
- <http://www.opengovdata.org/home/8principles>
- <http://lab.linkeddata.deri.ie/2010/star-scheme-by-example>
- http://en.wikipedia.org/wiki/Uniform_resource_identifier
- <https://valitsus.ee/UserFiles/valitsus/et/valitsus/tegevusprogramm/valitsustegevusprogramm/Valitsusliidu%20programm%202011-2015.pdf>
- <http://www.opendata.ee>
- <https://www.riigiteataja.ee/akt/122032011010?leiaKehtiv>

Avaandmete varamu



UUNO VALLNER

uuno.vallner@riso.ee
Majandus- ja Kommunikatsiooniministeerium



TANEL TAMMET

tammet@staff.ttu.ee
Tallinna Tehnikaülikool



ALEKSANDER REITSAKAS

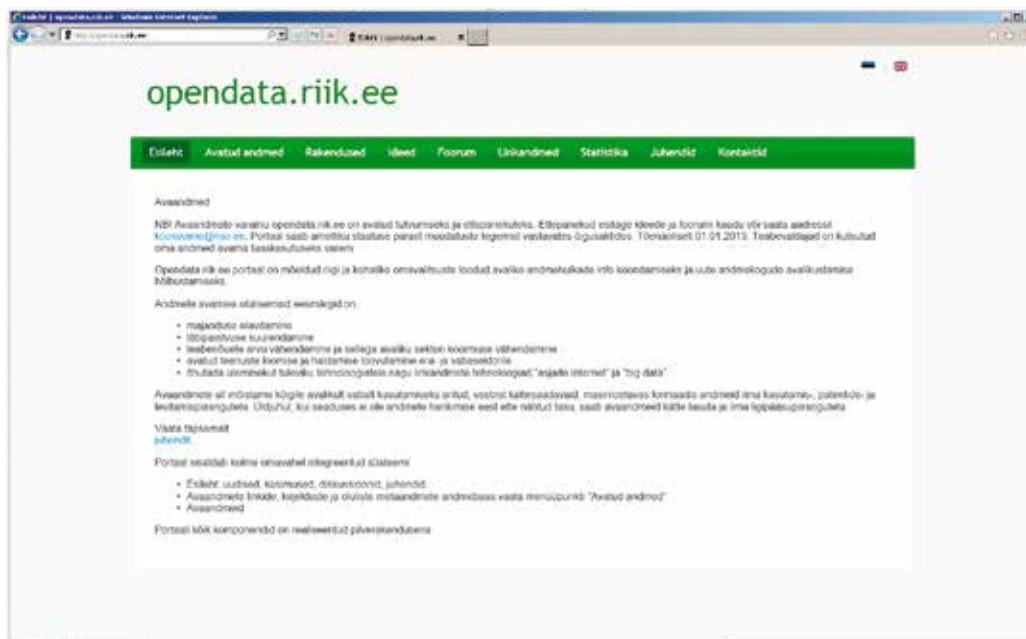
aleksander.reitsakas@aktors.ee
Aktors OÜ

Avaandmete kättesaadavuse parandamiseks ja avalikustamise koordineerimiseks on pilootrakendusena loodud avaandmete varamu <http://opendata.riik.ee>. Sinna peaks üles laaditama avaliku sektori avaandmete andmehulkade metaandmed. Varamusse võib asutus salvestada soovi korral lisaks ka andmehulga.

Avaandmete varamu

Avaandmete vaatenurgast vajab Eesti avalik sektor eelkõige muudatusi seadusandluses, organisatsiooniliste ja tehniliste põhimõtete kokkuleppimist. Seetõttu algatati aastateks 2011–2012 projekt „Avaandmete raamistik“. Projekti raames korraldati hange, mille eesmärk oli luua andmete avamist toetav infrastruktuur ja organisatsioonilised, tehnilised ning semantilised eeldused andmete avamisele. Hanke tulemuseks planeeriti:

- luua veebisait opendata.riik.ee (beeta) kui Eesti teabevärv avaandmetele juurdepääsuks ja kasutamiseks;
- luua andmete publitseerimise infrastruktuur (varamu, beeta);
- koostöös avaandmete kogukondadega fikseerida esialgsed organisatsioonilised, tehnilised ja semantilised nõuded andmete avamisele;
- keskseks varamuks soovitati pilvelahendust CKANi (<http://ckan.net>) baasil;
- eessüsteemina soovitati pilvelahendusel Drupali veebimootorit (<http://drupal.org>);
- otsimootoriks soovitati Apache SOLRi (<http://lucene.apache.org/solr>);
- eeldati linkandmete RDFi ja SPARQLi standardeid toetavaid liideseid;



Avaandmete portaali pilootrakenduse esileht

- eeldati LAMPi platvormi;
- nõuti suhtlemisvõimet teiste varamutega;
- eeldati, et asutused võivad luua oma varamuid, keskvaramu peaks olema võimeline metaandmeid nendest noppima;
- eeldati, et asutused võivad panna andmehulki otse kesksesse varamusse.

Avaandmete koondportaali pilootrakendus on aadressil <http://opendata.riik.ee>. Portaal kujutab endast kolme integreeritud süsteemi.

- Uudiste, küsimuste, diskussioonide ja juhendite portaal, kus esitada juhendeid ja uudiseid, tõstatada küsimusi ja diskuteerida avaandmete teemal.
- CKANI-põhine avaandmete linkide, kirjelduste ja oluliste metaandmete andmebaas (vt <http://ckan.org>), millele viib portaali ülariiba menüüpunkt „Avatud andmed“. Sellest andmebaasist saab:
 - 1) otsida ja alla laadida avaandmeid ligipääsupiiranguteta,
 - 2) lisada uusi avaandmeid (selleks on vaja portaali registreeruda ja saada haldaja käest ligipääsõigus).
- Andmehulkade hoidla, mis on üks võimalikest kohtadest, kuhu ametkond saab avaandmeid salvestada.

Tehniliselt on loodud eeldused avaandmete infrastruktuuri väljakujundamiseks. Kuid tehnilistest eeldustest on vähe. On vaja mehitada ja välja

õpetada meeskond, kes oleks võimeline haldama ja arendama infrastruktuuri, tegema järelevalvet ja haarama oma tegevusega nii avaliku sektori andmetootjad kui ka teenuseid loovad avaandmete kogukonnad.

Avaandmete infrastruktuuri väljakujundamise eeldused on loodud.

Kuidas avalikustada?

Mis vormingus? Peamise põhimõttena arvestame, et palju parem on avaldada andmed ebamugavas kodeeringus kui jätta need esialgu avaldamata põhjusel, et millalgi on plaanis võtta ette kodeeringu täiustamine. Teiseks, avaldatud andmehulka saab edaspidi avaldada uues, paremas kodeeringus.

Soovitame avaandmete süsteemi kontekstis lähtuda vormingute ja kodeeringute kasutajasõbralikkuse hindamisel Tim Berners-Lee viie täрни süsteemi¹ põhimõtetest, mis on kirjeldatud eelmises artiklis. Andmehulga avaldamiseks sobivad eeskätt vormingud, mida on võimalik avada ja töödelda vabavaraliste rakendustega. Selliselt on töödeldavad näiteks odt-vormingus dokumendifailid, samuti struktuursete andmete levinuimad vormingud .csv, .json, .xml.

Taaskasutamiseks sobivad vabavaraliste rakendustega avatavad ja töödeldavad vormingud. >>>

» **Ühetärni-vormingute** kasutamist andmete avamiseks peaks vältima. Kuid teiselt poolt on nende publitseerimine siiski kindlasti parem kui sellest loobumine.

Kahetärni-vorminguid kasutatakse eelkõige selliste andmete jaoks, kus kasutajale piisab juurdepääsust andmetele. Taaskasutamine tähendab eelkõige tutvumist andmetega ja nende kasutamist lõika-keebi meetoditega. Teenuste loomise tagamiseks tuleks avaandmed esitada kas kolme-, nelja- või viietärni-vormingus.

Kolmetärni-vormingud. Kolmetärni-andmed võiks olla ühel järgmistest vormingutest vastavalt sellele, mis on andmete avaldajale mugavam.

Loodud on avaandmete infrastruktuuri väljakujundamise eeldused.

Kasutaja seisukohast ei ole neil vormingutel väga olulist vahet, kuid kõige mugavam on tõenäoliselt kasutada json-vormingut.

- csv-failid. Dokumentatsioonis peab olema öeldud tähestiku kodeering ja koma/semikooloni ning komaga arvu eraldaja (punkt/koma) kasutus. Soovitav on kasutada failides päisereas, kus väljade nimed on toodud selles päisereas. Kindlasti tuleks lähtuda ametlikust² csv-vormingust koos nüanssidega jutumärkide teemal jne.
- json-vormingus failid, samad nõuded tähestiku kodeeringu kohta.
- xml-vormingus failid.

Neljatärni-vormingud. Põhimõtted on samad kui kolmetärni-andmetel, kuid peamise täiendusena kasutatakse objektide identifitseerimiseks globaalselt unikaalseid identifikaatoreid ehk URIsid. Globaalsete identifikaatorite kasutus muudab andmete ristkasutuse teistes süsteemides oluliselt mugavamaks.

URId e kasutuselevõtuks tuleb andmete ekspordi ajal lisada igale objekti-identifikaatorile antud andmehulga prefiks, näiteks <http://asutus.ee/andmehulganimi/objects/>, kus siis terve URI oleks näiteks <http://asutus.ee/andmehulganimi/objects/45321> ja 45321 on objekti algne ID andmehulgas. Kui IDd ei ole ka andmehulga enda lõikes unikaalsed (mis on kõige harilikum olukord), siis kõige lihtsam on esitada ekspordimisel URId kujul, kuhu lisatakse objects-i asemel

vastava tabeli nimi, näiteks <http://asutus.ee/andmehulganimi/isikud/45321>.

Kui objekte on asunud esitada URIdena, siis on sobiv lisaks csv/json-i/xml-i kasutamisele esitada andmeid RDFi kujul objekt-omadus-väärtus kolmikutena³.

Kuna RDFi kujul saab andmeid esitada eri süntaksitega, soovime kasutada üht järgmistest kahest.

- Microdata kujul⁴, mis on ette nähtud andmete kodeerimiseks inimloetava html-i sisse: info on korraga nii harilikul viisil inimloetav kui ka kergesti masintöödeldav.
- RDFa⁵, mis on analoogiline ja samade eesmärkidega kui Microdata, kuid veidi keerukam.

Microdatas esitatud andmed on alati triviaalselt konverteeritavad RDFaks. Järgmine küsimus peale Microdata/RDFa teemat on väljanime ehk objekti omaduste nimede valik. Siin on kaks peamist lähenemist.

Microdatas esitatud andmed on alati triviaalselt konverteeritavad RDFaks. Järgmine küsimus peale Microdata/RDFa teemat on väljanime ehk objekti omaduste nimede valik. Siin on kaks peamist lähenemist.

- Kõige lihtsam on esitada algse andmehulga tabeli/väljanime paarid URIdena, näiteks kujul <http://www.asutus.ee/andmehulganimi/tabelinimi/väljanimi>, kus näide võiks olla <http://www.asutus.ee/loasaajad/fyysisikud/synniaeg>.
- Veidi keerulisem, kuid kohati kasulik alternatiiv on kasutada algse süsteemi tabeli/väljanime asemel üldisemat ja laiemalt levinud omaduse nime, kui sellise leiab. Sobivaks kataloogiks nimede otsimisel on schema.org. Tasub tähele panna, et kui sobivat nime ei leita, on kasutajal hiljem siiski väga lihtne teistendada eksporditud nimesid endale sobivale kujule, eeldusel, et ta saab eksporditud väljanime tähendusest sisuliselt aru.

Väljanime esitamisest rääkides tasub puudutada ka ontoloogiate teemat. Neid võib vaadelda kui väljanime teisendus-/klassifitseerimisreeglid, näiteks, kui soovime öelda, et meie URI kujul väljanimi <http://www.asutus.ee/loasaajad/fyysisikud/synniaeg> on täpselt sama asi kui [schema.org-i Thing](http://schema.org/Thing)>Person>birthDate.

Selliselt vaadates ei ole ontoloogiad andmete avalikustamisel otseselt oluline ega keeruline teema, pigem on tegu kasuliku töövahendiga rakenduste loojatele, kes kombineerivad eri allikatest saadud andmeid. Andmete ekspordimiseks avalikustamisel tasubki ontoloogiad soovi korral ise kirjutada

kas siis oma väljanimed dokumenteerimiseks või alamhulga olemasolevate väljanimed konverteerimiseks schema.org-i nimedeks.

Viietärni-vormingute selgitusi. Andmete URIde kaudu linkimise üks viise on kasutada andmebaasis rakendatava identifikaatori asemel võimaluse korral *de facto* universaalsemat globaalset identifikaatorit ehk URI. Oletame näiteks, et riigis lepatakse kokku (või asuvad näiteks rahvastikuregister ja äriregister kasutama) isikukoodide ja ettevõtete koodide jaoks vormingut kujul <http://prefiks1.ee/prefiks2/isikukood> ja <http://prefiks3.ee/prefiks4/ettevottekood>. Sel juhul oleks isikukoodi ja ettevõtte koodi viietärni-esituseks taolisel kujul URId, kus prefiks / URI kujud ei ole mitte antud asutuse enda, vaid üldisemalt kokkulepitud / laiemalt kasutusel kujud. Sama kehtib siis ka andmebaasiväljade ehk objektide omaduste nimede kohta.

Kuidas andmehulka reaalselt avalikustada? Konkreetselt on andmete avalikustamiseks kolm peamist tehnoloogilist viisi.

- Inimloetavate failide korral pakkida faile sisaldavad kataloogid kokku, lisada peakataloogi lühike sisuseletus ja laadida pakitud kataloog/kataloogid vabalt allatõmmatavana soovitatavalt asutuse veebisaiti <http://<asutuse domeeninimi>.ee/avaandmed> või opendata.riik.ee kataloogi.
- Andmebaasides sisalduvate andmete korral eksportida andmebaasi sisu kas xml-, või csv- või json-failideks vms struktureeritud tekstikujule ning rakendada seejärel sama lihtsat kokkupakkimise ja veebiserverisse laadimise meetodit. Kui andmebaas sisaldab isikuand-

meid, mis ei kuulu avalikustamisele, siis neid väljasid lihtsalt ei ekspordita.

- Alternatiivina võib andmebaasides esitavad andmed avalikustada vabalt kasutatava võrguteenusena, mille kaudu on võimalik leida ja alla laadida kogu andmehulga sisu või selle filtreeritud osahulk. Võrguteenus võib olla näiteks SOAP-teenus, kuid eelistatumad on lihtsamad, näiteks jsoni-põhised nn REST-teenused, samuti näiteks ka lihtsalt csv-vormingusse välja andvad get- või post-sisendparameetritega teenused.

Andmed peavad olema mõistlikult kirjeldatud, st nende eesmärgist, struktuurist ja sisust peab andmehulgaga varem mitte kokku puutunud, kuid siiski valdkonda ja tehnoloogiat mõistev inimene mõistliku pingutusega iseseisvalt aru saama.

Andmehulga edaspidise uuendamise põhimõtted ja uuendamise planeeritav sagedus peavad olema andmehulga juures kirjeldatud. Andmehulga avaldajal ei lasu seejuures mingit otsest kohustust andmehulka regulaarselt uuendada – tähtis on uuendamise kava (või selle puudumine) arusaadavalt kirja panna.

Asutuse avalikustatud andmehulgad peavad olema kergesti leitavad. Selleks tuleb kasutada vähemalt kaht viisi avalikustatud andmete olemasolu, kirjelduste ja laadimislinkide avaldamiseks.

- Asutuse oma veebisaidil spetsiaalne kataloog/avaandmed, näiteks <http://www.asutus.ee/avaandmed>
- Üleriiklik avaandmete koondportaal/varamu <http://opendata.riik.ee>



1 <http://lab.linkeddata.deri.ie/2010/star-scheme-by-example>

2 http://en.wikipedia.org/wiki/Comma-separated_values

3 http://en.wikipedia.org/wiki/Resource_Description_Framework

4 http://en.wikipedia.org/wiki/Microdata_%28HTML%29

5 <http://en.wikipedia.org/wiki/RDFa>

Avatud ruumiandmed



KRISTIAN TEITER

kristian.teiter@maaamet.ee
Maa-amet

Mis on ruumiandmed?

Ruumiandmed on lihtsustatult öeldes andmed, millel on geograafiline asukoht ja kuju. Selliseid andmeid nimetatakse ka geoandmeteks, geoinfoks ja asukohaandmeteks. Reeglina esitatakse ja kasutatakse ruumiandmeid kaardina, mida võib lugeda ka andmekogu ruumiandmete väljundiks. Näiteks Eesti topograafia andmekogus hallatavate topograafiliste andmete üheks väljundiks on topograafilised kaardid, kuid andmeid endid saab kasutada ja kättesaadavaks teha ka näiteks veebiteenuste kaudu xml-kujul.

Valdkonnad, kus ruumiandmeid põhiliselt kasutatakse, on keskkonnakaitse, planeerimine, ehitus, logistika ja transport, sõjandus, statistika jne. Järjest enam osatakse näha asukohas peituvat potentsiaali ning ruumiandmete kasutamine eri eluvaldkondades kasvab plahvatuslikult.

Ruumiandmete hulka kuuluvad ka aadressiandmed. Ilmselt on nii mõnelegi andmekogu haldajale viimasel ajal just tänu aadressiandmetele jõudnud üllatusena kohale teadmine, et tema hallatav andmekogu sisaldab ruumiandmeid.

Avalikustamine ja taaskasutamine

Võrreldes Euroopa ja maailmaga on ruumiandmed, mida saab käsitleda avaliku teabena, Eestis hästi avalikustatud. Maa-amet kui suurim riiklik kaarditootja ja ruumiandmete haldaja avalikustas juba 2001. aastal katastriüksuste andmed, halduspiirid ja topograafilised aluskaardid veebipõhise kaardiserveri (<http://geoportaal.maaamet.ee/>) kaudu. 2008. aastal lisandusid avalikule kaardiserverile veebipõhised kaarditeenused

(WMS), mille kaudu on Maa-ameti kaardid kasutatavad mitmesuguste GIS-/CAD-tarkvarade abil. Kaardiserver ja teenused on väga populaarsed, kokku tehakse nende abil umbes 500 000 külastust kuus.

Teise näitena võib esile tõsta Keskkonnateabe Keskuse, mille kodulehelt näeb interaktiivsete kaardiserverite kaudu igasuguseid keskkonnateemalisi ruumiandmeid. Üheks näiteks on metsaregistri avalik veebiteenus.

Avalikustamise ja taaskasutamise vahe on valdavalt selles, et avalikustatud ruumiandmeid saab vaadata, pärida, otsida ning piiratud ulatusega pildina ka alla laadida ja välja trükkida. Taaskasutataval kujul ruumiandmete kasutusvõimalused on aga piiramatud ning reeglina on need andmekogumitena sobivas vormingus allalaaditavad. Just taaskasutataval kujul ruumiandmete kättesaadavaks tegemine loob eeldused, et era- ja kolmas sektor kasutavad avaliku sektori teavet uute ja huvitavate teenuste ning rakenduste loomiseks.

Taaskasutataval kujul ruumiandmete kättesaadavusega on Eestis pilt üsna kirju. On ruumiandmeid, mis on taaskasutataval kujul kogu Eesti kohta lihtsalt kättesaadavad, kuid on ka selliseid, mille kättesaadavus on mitmel põhjusel keeruline. Andmete kättesaadavus on erinev nii ametkondade vahel kui ka nende sees.

Vastavus avatud andmete põhimõtetele

Olen siin ära toonud oma subjektiivse hinnangu Eesti ruumiandmete olukorra vastavuse kohta

mõnele avatud andmete põhimõttele. Kuid asjaolu, et tegemist on ruumiandmetega, ei oma selles olukorras mingit erilist tähtsust. Pigem on pilti mõjutanud andmekogude haldajate tehnoloogiline võimekus, õiguslik regulatsioon, ajaloolised tavad jmt tegurid.

Üheks põhimõtteks on see, et andmed on töötletud kogutud algallikast ja need on säilitanud originaalkuju ja detailsuse. See on põhimõte, millega oli ruumiandmete osas rohkem probleeme 10–15 aastat tagasi, kuid tänapäeval reeglina enam mitte. Ruumiandmete kasutajatel läks aega, kuni nad aru said, et kasutades teabevaldajate ruumiandmeid, on nende endi huvides, et need oleksid pärit algallikast ja ajakohased. Paradoksaalsel kombel võib avatud andmete poliitika rakendumine Eestis seda olukorda hoopis suurel määral halvemaks muuta. Kolmanda osapoole ehk arendaja tehtud rakenduste kasutamisel ei ole lõppkasutajal enam sidet andmete tootjaga ehk algallikaga. Samuti ei ole teada, kuivõrd erinevad on lõppkasutajale nähtavad ruumiandmed nendest andmetest, mida arendaja sai algallikast. Avatud andmete poliitika väljatöötajad muretsevad küll selle pärast, et kõigile huvilistele ehk arendajatele ja lisaväärtuse tootjatele oleksid andmed, sh ruumiandmed, kättesaadavad algallikast, kuid see, mis saab nendest ruumiandmetest pärast arendajapoolset töötlust ja edasimüümist, pole kuidagi paika pandud. Ilmselt hakkab seda reguleerima turg ja lõppkasutajate teadlikkus.

Mainimisvääreteks põhimõteteks on andmete masinloetavus, ajakohasus ja vabade standardite kasutamine. Tegemist on põhimõtetelega, millele vastavust on võimalik suuresti tagada tehniliste meetmetega. Kuna Eestis hakati paljusid ruumiandmeid sisaldavaid andmekogusid pidama alles 20 aastat tagasi, on need hallatavad masinloetaval kujul, mitte aga skaneeritud ajalooliste dokumentide kogumitena. See on suur erinevus ja eelis võrreldes Lääne-Euroopa riikidega, kes on pidanud kulutama märkimisväärseid ressursse kaartide digitaliseerimisele ja vektoriseerimisele. Ruumiandmete ajakohasuse tagamiseks teabevaldaja andmekogu ning koha vahel, kus ruumiandmed on taaskasutataval kujul kättesaadavad, on ilmselt abi rajatavast riigi avaandmete koondportaalist ning andmete kasutaja võib olla kindel, et need andmed, mis ta alla laadis, on samasugused ka teabevaldaja andmekogus. Hoopis valusam on aga ruumiandmete puhul

küsimus, kas teabevaldaja andmekogus olevad andmed on ajakohased ja vastavad reaalsusele. Avatud andmete puhul peetakse oluliseks põhimõtet, et need oleksid esitatud vabas vormingus, mis ei ole ühegi ettevõtte ega isiku ainuomand. Rääkides ruumiandmete kasutajate vajadustest Eestis, tuleb mainida, et kasutajad soovivad saada andmeid vormingus, mida „sööv” nende kasutatav GIS-/CAD-tarkvara. Ruumiandmete konverteerimine ühest vormingust teise on rahulolematust põhjustav ebamugavus, isegi kui tarkvara seda võimaldab. Eestis kasutatakse nii kindlate tootjate GIS-tarkvara kui ka vabavara GIS-tarkvara, mis on siiski vähem levinud. Seega

Avatud andmete poliitika rakendamine kujuneb efektiivseks, kui suudetakse üleriiklikult ühtlustada taaskasutataval kujul avaliku teabe ligipääsu, väljastamise ja kasutustingimused ning tasu võtmise põhimõtted.

peaksid avatud ruumiandmed olema kättesaadavad vormingutes, mida valdavalt kasutatakse, sh nii mõnes tootjakeskses ja suletud kui ka vabas vormingus.

Viimase grupina võib välja tuua avatud andmete põhimõtted, mis käsitlevad andmete kasutamise õigusi, piiranguid ning kättesaadavust. Mitmel põhjusel on need aspektid ruumiandmete kättesaadavuse osas Eestis üpris ebaühtlaselt reguleeritud. Avaliku teabe seadusega on kehtestatud ühtsed andmete avalikustamise põhimõtted. Ruumiandmete osas reguleerib nende kättesaadavuse küsimusi ruumiandmete seadus, milles kajastuvad INSPIRE direktiivi põhimõtted. Ruumiandmete seadus kohustab teabevaldajaid tegema nende hallatavad ruumiandmed kättesaadavaks kindlatele nõuetele vastavate teenuste, sh allalaadimisteenuste kaudu ning kujul, mis vastab samuti kindlatele nõuetele. Samas jätab ruumiandmete seadus teenuste jagamise tingimused ja korra ehk andmete kasutusõigusi ja litsentseerimist puudutavad küsimused reguleerimata ning annab volitused ministrile, kelle valitsemisalasse vastav andmekogu kuulub.

Suures osas on andmete kasutamist puudutavaid küsimusi reguleeritud vastavates õigusaktides. Nii et põhimõtted, mis puudutavad andme-»

» kogust andmete taotlemise, väljastamise ning andmete kasutamise tingimusi, on sätestatud paljudes õigusaktides, milles orienteerumine on keeruline.

Raha

Kas avalik teave peaks taaskasutataval kujul olema kõigile tasuta kättesaadav või peaks selle eest siiski maksma? Kui suur võib olla tasu? Need küsimused on ilmselt kirglikeks aruteluteemadeks nii Eestis kui ka kogu Euroopa Liidus ning aktuaalsed ka ruumiandmeid haldavate teabevaldajate hulgas.

Teabevaldajatele on Eestis teiste teabevaldajate ruumiandmed tasuta kättesaadavad. Olukord on aga kirju andmete tasudega era- ja kolmandale sektorile. Kui üldistada (ja mitte eristada, mille eest täpselt tasu võetakse, kas teenuse osutamise, ruumiandmete väljastamise toiming, ruumiandmete kasutusse andmise või muu taolise eest), siis võib ütelda, et tasu võtmine ja tasumäärad on andmekoguti erinevad. Näiteks kehtestab ruumiandmete seadus tasud Eesti topograafia andmekogu andmetele, kuid teatud keskkonnanalased andmed, nagu metsaregistri andmed, on keskkonnateabe keskuse kodulehelt vabalt allalaaditavad. Või näiteks aadressiandmed on Maa-ametist kõigile taaskasutataval kujul tasuta kättesaadavad, kuid katastriüksuste andmete väljastamisele kehtestab tasud riigilõivuseadus.

Selline olukord on tekkinud üpris pika aja jooksul ning see pole iseloomulik ainult ruumiandmetele, vaid kõikidele avaliku sektori andmetele. Võib

spekuleerida, et teatud andmekogude puhul on tajutud monopoolset seisundit ning pole jäetud kasutamata võimalust toiminguid riigilõivustada. Teatud andmekogude puhul on aga teabevaldaja ja riigi huvides, et andmed ühiskonnas laiemat kasutust leiaks – sel juhul on need tasuta ja võimalikult lihtsalt kättesaadavad.

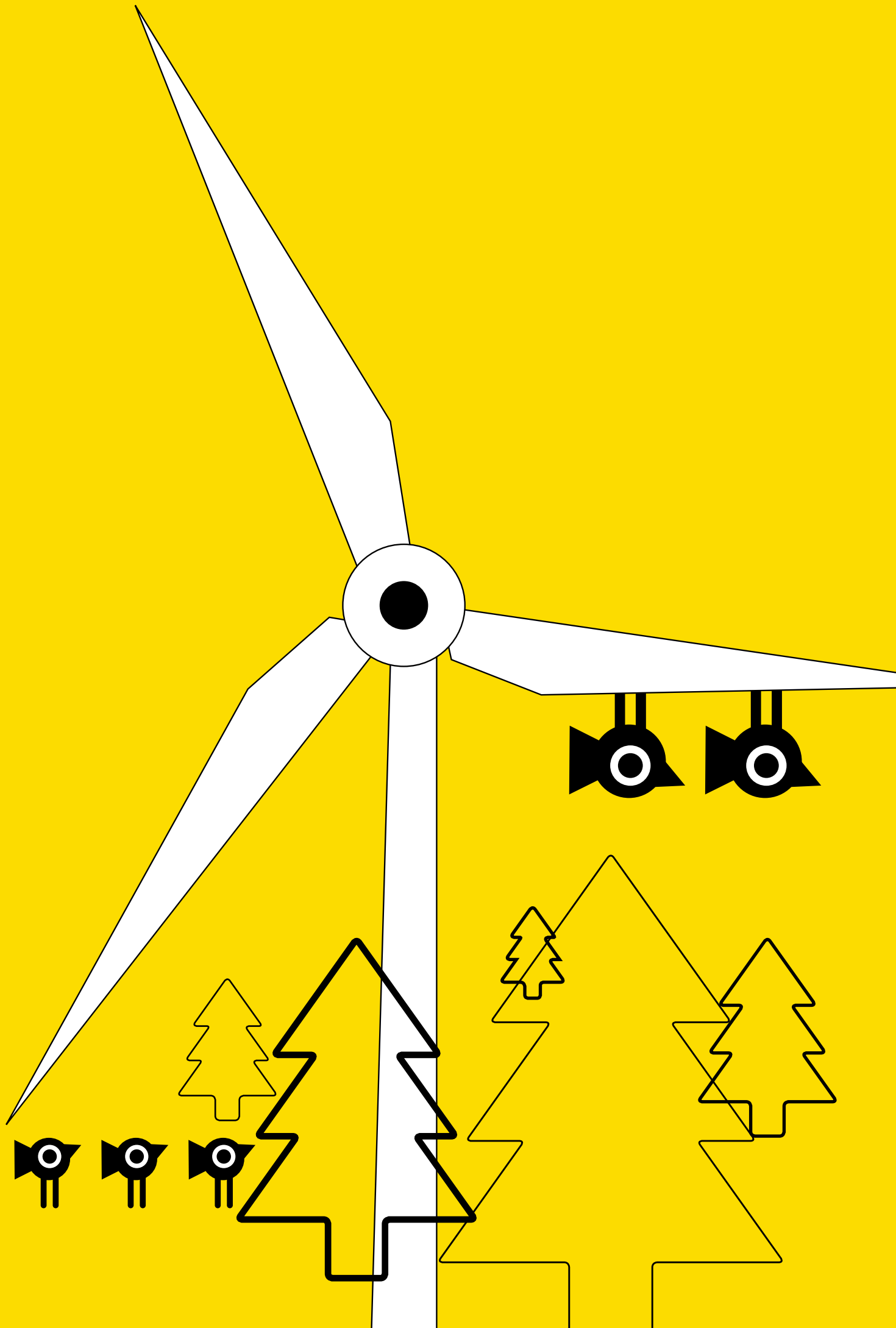
Ka teistes Euroopa riikides on olukord erinev. Näiteks sõltub väga palju sellest, kui suurel määral finantseeritakse teabevaldajaid riigieelarvest ning kui suures mahus peavad nad ise raha teenima. Markantseks näiteks on PSI direktiivi täiendamise eelnõu sõnastus, mis puudutab tasusid. Ilmselt on üritatud leida kompromissi vastandlike huvide vahel ning tulemuseks on sõnastus, mis jätab mitmeteks tõlgendusteks laialdased võimalused.

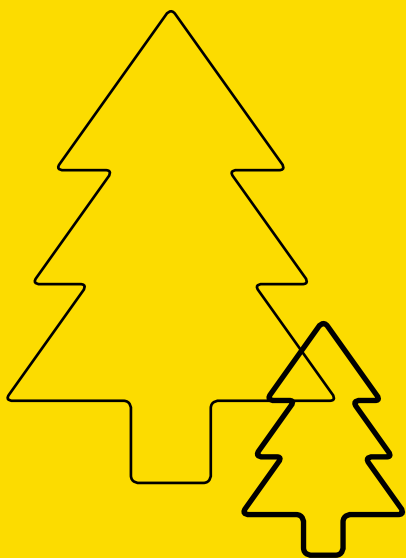
Kokkuvõtteks

Avatud andmete poliitika rakendamine kujuneb efektiivseks, kui suudetakse üleriiklikult ühtlustada taaskasutataval kujul avaliku teabe ligipääsu, väljastamise ja kasutustingimused ning tasu võtmise põhimõtted. Praegu läheb palju jõudu tehnilise infrastruktuuri rajamise peale, mis soodustaks andmete taaskasutataval kujul kättesaadavaks muutmist. Kuid ainuüksi sellest ei piisa ning võib eeldada, et plahvatuslikku muudatust taaskasutataval kujul andmete kättesaadavuse osas lähiajal ei toimu. Kas see on edasimineku või paigalseis, sõltub juba sellest, millise mätta otsust vaadata. Vähemalt ruumiandmed on viimaste aastate jooksul muutunud järjest avatumaks ning selline trend jätkub.









2. PEATÜKK

ROHELINE IT

Oleme silmitsi olukorraga, kus loodusressursid vähenevad üha ning ligipääs neile on muutunud keeruliseks, ent samas vajavad riigid neid kasvu tagamiseks üha enam. Seega eeldab majanduse konkurentsivõime tõstmine nutikamat ja ressursitõhusamat tootmist ning tarkade tehnoloogiate kasutuselevõttu. OECD peab jätkusuutliku majanduse üheks võtmekomponendiks IKT-d, viidates, et samas kui IKT-sektor tekitab 2% maailma süsihappegaasist, suudab see vähendada ülejäänud 98% CO₂ tekitajate negatiivset mõju. See peatükk annab ülevaate Eesti rohelise IKT potentsiaali kaardistamiseks läbi viidud uuringu tulemustest, samuti plaanidest, kuidas selle käigus antud soovitusi ellu rakendada. Lisaks avaliku sektori plaanidele antakse ülevaade ka erasektori toimetamistest: ambitsioonikast Targa Vormsi algatusest ning e-veoselehe projektist.



Roheline IKT kui keskkonnasäästu ja kulude kokkuhoiu võimaldaja



KRISTIINA KITSIK

kristiina.kitsik@mkm.ee

Majandus- ja Kommunikatsiooniministeerium

2011. aasta lõpus korraldas Majandus- ja Kommunikatsiooniministeerium koostöös Ernst & Youngiga uuringu Eesti ettevõtjate roheline IKT alase teadlikkuse ning selle valdkonna potentsiaali kaardistamiseks Eestis.

Roheline IKT on 21. sajandi alguses välja kujunenud kontseptsioon, mis ühendab endas IKT lahendused ja keskkonnasäästu. Suures plaanis tegeleb roheline IKT kahe põhivaldkonnaga: IKT seadmete ja lahenduste keskkonnasäästlikkusega (IKT rohelineks muutmine) ning muude eluvaldkondade keskkonnasäästlikkuse tõstmisega IKT lahenduste abil (selle abil rohelineks muutmine). Kui varem peeti keskkonnahoiu temaatikat vaid roheline liikumise pärusmaaks, siis koos IKT lahenduste arenguga põimub see üha enam ettevõtete igapäevasesse tegevusse. Selle põhjuseks on asjaolu, et ühelt poolt võimaldab IKT saavutada kulude kokkuhoiu tööprotsessides ja teisalt on paljudele ettevõtetele ärivõimaluseks uute toodete ja teenuste arendamisel.

Uuringust „The role of green ICT in enabling smart growth in Estonia“¹ selgub, et Eesti ettevõtted teadvustavad IKT lahenduste rolli ja otsivad roheline IKT abil võimalusi tootmisprotsesside efektiivsemaks ja keskkonnasõbralikumaks

muutmiseks. Valdavalt on selliste lahenduste kasutuselevõtt motiveeritud soovist raha kokku hoida, kuigi oluliseks peetakse ka keskkonnasäästlikkust iseenesest.

Rohelise IKT lahendusi võib leida paljudest eluvaldkondadest. Hoonete energiaefektiivsuse osas võib näitena välja tuua Eesti ettevõtte Yoga nn targa maja lahenduse. Ettevõtte enda hinnangul võimaldab nende lahendus hoone küttekulusid vähendada kuni 30%. Transpordivaldkonnas kasutatakse IKT lahendusi veokite marsruutide optimeerimisel. Eesti suuremad telekommunikatsiooniettevõtted EMT ja Elion piloteerivad lahendusi, millega kasutatakse serveriruumides ülejäävat soojusenergiat ümberkaudsete kontori- ja eluhoonete kütmiseks. Aktiivne kogukond veab Smart Vormsi projekti, mille eesmärk on parandada IT lahenduste abil väikesaare elanike elukeskkonda (loe lk 32).

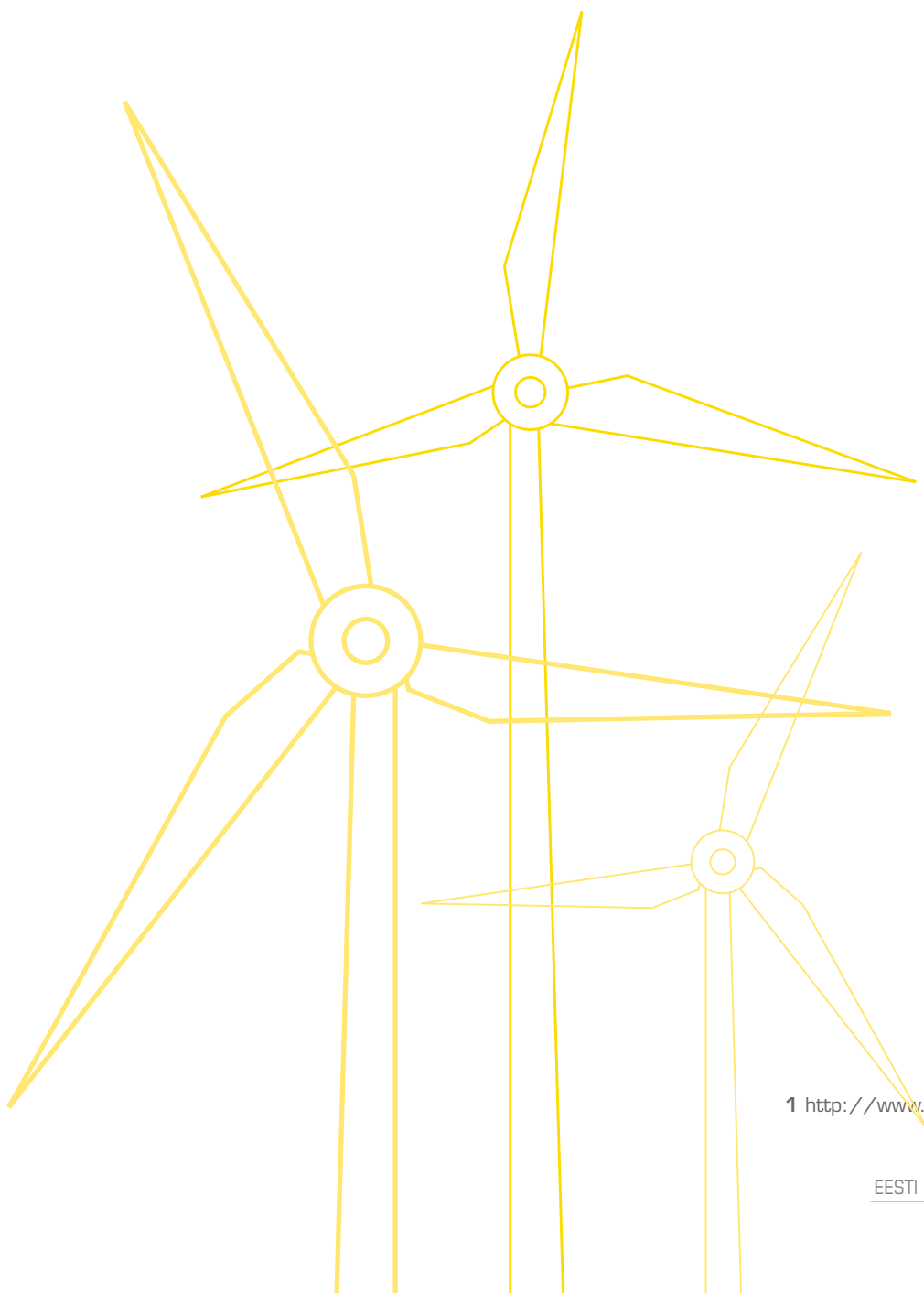
Lisaks pakub ressursisäästu tavapäraste paberdokumentide ja kontorite külastamist nõudvate teenuste asendamine e-teenuste ja tarkvaralahendustega. Kuigi selles osas on Eestis aktiivne roll olnud riigisektoril (ID-kaart, X-tee, e-tervis, e-kool, e-maksuamet jne), leiab häid näiteid ka erasektorist, näiteks internetipangandus ja mo-

biiliparkimine on rohelise IKT lahendused, mis on meil kasutusel juba üle 10 aasta.

Vaatamata mõnele heale näitele tuleb tõdeda, et suures osas on rohelise IKT lahenduste kasutuselevõtt ja väljatöötamine Eestis alles piloteerimisjärgus. Uuringu käigus küsiti ettevõtetelt, milliseid takistusi nad rohelise IKT kasutuselevõtul näevad. Ootuspäraselt toodi suurima takistusena välja rahalisi piiranguid (ca 85% vastanutest) – tehnoloogia arendamine ja innovatsioon on kulukas. Sageli vajavad intelligentsed rohelise IKT lahendused suurt alginvesteeringut ning pakuvad kokkuhoidu pigem ülalpidamiskuludelt. Toodi ka välja, et puudub usaldusväärne metoodika rohe-

lise IKT lahenduste tasuvuse väljaselgitamiseks. Seetõttu jäävad ettevõtted sageli rohelise IKT lahenduste osas äraootavale seisukohale. Sarnase probleemi ees seisavad ka avaliku sektori asutused, kes riigihangete seadusest tulenevalt on sunnitud kokku hoidma pigem soetuskuludelt.

Ernst & Youngi ning Majandus- ja Kommunikatsiooniministeeriumi uuring toob välja poliitika-soovitused rohelise IKT valdkonna arengut takistavate piirangute ületamiseks. Uuringu tulemused on olnud allikaks ministeeriumi programmile, mille raames plaanitakse toetada rohelise IKT lahendusi.



¹ http://www.mkm.ee/public/Inno_18_GreenICT.pdf

Ökoinnovatsiooni toetamine IKT lahenduste abil



KRISTIINA KITSIK

kristiina.kitsik@mkm.ee

Majandus- ja Kommunikatsiooniministeerium

Eelmises artiklis oli lähemalt juttu Majandus- ja Kommunikatsiooniministeeriumi tellimusel Ernst & Young Balticu korraldatud rohelise IT uuringust „The Role of Green ICT in Enabling Smart Growth in Estonia“¹, mille eesmärk oli välja selgitada rohelise IKT alase teadlikkuse tase ning potentsiaal Eestis. Muuhulgas esitati riigile poliitikasoovitused. Siin on peamised neist.

Rohkem tuleks panustada rohelise IKT alase teadlikkuse tõstmisse. Kuigi Eesti on võrreldes teiste ümberkaudsete riikidega IKTs eesrindlik ning meil on selles vallas häid näiteid kasutusel olevatest lahendustest, siis suures plaanis võib väita, et tegelikult ei teadvustata, et uute IKT lahenduste loomise või sisseostmise abil on võimalik säästa mitmeid ressursse: energiat, aega, raha, materjale jne.

Kuidas teadlikkust tõsta?

- Luua avalikult kasutatav rohelise IKT lahenduste ja toodete andmebaas.
- Pakkuda (nt EASi ja Arengufondi poolt) rohkem ärikonsultatsioone, mille eesmärgiks on selgitada roheliste tehnoloogiate ja rohelise IKT potentsiaali.
- Tuua näited juba praegu kasutusel olevatest lahendustest.
- Tunnustada mõnel ettevõtluskonkursil ettevõtjaid rohelise IKT eriauhinnaga.

Toetada koostööd sidusrühmade ning fookusvaldkondades tegutsevate ettevõtete vahel. Koos-

töö suurendaks sünergiasid ning tugevdaks ettevõtete konkurentsivõimet.

Lahendused.

- Teha rohkem era- ja avaliku sektori ühisprojekte.
- Integreerida rohelise IKT teema klasteritesse või aidata kaasa rohelise IKT alase klasteri tekkimisele.
- Selgitada välja täpsemad koostöövõimalused ning saadav kasu.

Rahaline toetus rohelise IKT lahendustele.

See omakorda kiirendaks nende kasutuselevõttu ettevõtetes ja ühiskonnas.

Nimetatud probleeme aitab lahendada uus välja-töötamisel olev programm „Keskkonnasõbraliku innovatsiooni arendamine IKT abil“². Seda rahastatakse Norra finantsmehhanismist 2009–2014 ja töötatakse välja tihedas koostöös programmi partneri Innovation Norwayga.

Programmi kujundamisel on lähtutud kahest riikliku tasandi strateegiast: „Eesti teadus- ja arendustegevuse ning innovatsiooni strateegiast 2007–2013“ ja „Infoühiskonna arengukava 2013 rakendusplaanist 2012–2013“. Kuid samas ka vajadusest ära kasutada IKTd ressursisäästuks ja uuteks nutikateks lahendusteks.

Programmi üldiseks eesmärgiks on suurendada Eesti keskkonnavalast, majanduslikku ja sotsiaal-

set jätkusuutlikkust, arendades nutikaid IT-lahendusi, mis aitaks ressursse säästa. See tähendab, et peaksime kõiki olulisi ressursse hakkama kasutama paremini ja eelkõige nii, et neid jätkuvalt kasutada aastasadadeks. Nutikad IT-lahendused on heaks abivahendiks selle eesmärgi saavutamisel. Aitavad need ju protsesse optimeerida ning efektiivsemaks muuta.

Programmi raames plaanitakse toetada ettevõtteid, mittetulundusühinguid ja sihtasutusi ning pakutakse tuge just keskkonnasäästlike innovaatiliste äriideede arendamiseks ja sisenemiseks rahvusvahelisele turule. Eelkõige on kriteeriumiks organisatsiooni soov luua uusi või arendada olemasolevaid lahendusi, mitte tema juriidiline vorm. Pigem näeme, et IKT lahenduste abil saavutatakse ressursisääst järgmistes riiklikes strateegiates seatud valdkondades: transport ja logistika, energeetika, tööstus ja tootmine ning e-tervis.

Kokkuvõttes peaks programmi tulemusena suurenema eelkõige uute ja uudsete IKT lahenduste hulk ja kasutuselevõtt ning kasvama ressursisääst. Ühtlasi peaks arenema ettevõtjate vaheline koostöö ning kasvama käive, eriti eksportkäive.

Kui suureneb Eesti ettevõtete nutikate IKT lahenduste baasil valminud uute (või uuendatud) teenuste ja toodete maht, toetab see kindlasti ühiskonna jätkusuutlikku arengut. Uute lahenduste või vanade uuendamise kaudu suureneb ka Eesti ettevõtete kompetents ja võimekus, mis omakorda tõstab konkurentsivõimet.

Head konkurentsieelised annavad aga võimaluse teha paremaid pakkumisi nii kohalikul kui ka rahvusvahelisel turul. Selleks et olla rahvusva-

helistel turgudel konkurentsivõimelisem, peavad ettevõtted tegema rohkem koostööd nii Eesti kui ka teiste arenenud riikide ettevõtetega. Seetõttu soodustame programmiga ka koostööd Norra ja Eesti vahel. Leiame, et meil on üksteiselt palju õppida ning üle võtta. Samuti arvame, et koostöö võimaldab läbi lüüa kolmandatel turgudel.

Programmi viime ellu koostöös MKMi allasutuse Ettevõtluse Arendamise Sihtasutusega (EAS), kelle peamiseks rolliks on toetuste andmine ning ettevõtete konsulteerimine.

Programm on jaotatud väiketoetuskeemiks ja põhitoetuskeemiks.

Väiketoetuskeem on mõeldud põhitoetuskeemi taotluste ettevalmistamiseks. Toetatakse järgmisi tegevusi: projektipartnerite otsimine Norrast, kaardistuste, uuringute, analüüside ja ekspertise tegemine, valdkondlike IKT lahenduste kontseptsioonide väljatöötamine, testimine ning arendamine ja valdkondlike koostöövõrgustike või muude koostöövormide algatamine, samuti konsultantide ja ekspertide kaasamine ettevõttes planeeritavate IT-lahenduste arendamisse.

Väiketoetuskeemist toetuse taotlemine ei ole eelduseks põhitoetuskeemi taotluse esitamiseks.

Põhitoetuskeemi voores oodatakse aga juba eluviidavaid suuri projekte. Eelkõige soovime näha projekte, mille raames valmib ressursisäästlik lahendus, millel on äripotentsiaal nii Eestis kui ka väljaspool.

Kogu programmi eelarve on 2012–2015 ligikaudu 7 miljonit eurot.



¹ http://www.mkm.ee/public/Inno_18_GreenICT.pdf



² <http://www.eas.ee/et/ettevotjale/innovatsioon/norra-eesti-koostoeoeprogramm-green-industry-innovation>

Nutikas Vormsi toob saarele taastuvenenergia ja kaugtöökohad



INDREK PETERSOO

indrek.petersoo@ericsson.com

Eesti Infotehnoloogia ja Telekommunikatsiooni Liit

Mittetulundusühingu Nutikas Vormsi eesmärgiks on Vormsi saare energiamajanduslikult iseseisvaks muutmine, kaasaegse elukeskkonna arendamine ja kohaliku majanduselu edendamine. Ettevõtmise eestvedajad loodavad oma kogemust ekspordida ka teistesse riikidesse.

Nutika Vormsi idee aluseks on viis aspekti: nutikad Vormsi inimesed, nutikas majandus, nutikas elukeskkond, mobiilsus ning saarel kättesaadavad avalikud teenused.

2011. aasta detsembris loodud MTÜ asutajateks olid Vormsi Vald, Net Group OÜ ja Volta AS. Koostööpartnerite ringi kuuluvad nii Vormsi saare elanikud, teised Eesti ettevõtjad, Tallinna Tehnikaülikool kui ka Majandus- ja Kommunikatsiooniministeerium. MTÜga on oodatud liituma kõik huvilised, kes soovivad unikaalsesse nutika väikesaare arendusse oma panuse anda.

Merekaablist sõltumatuks

MTÜ Nutikas Vormsi juhatuse liige Priit Kongo näeb saart tulevikus taastuvenenergia tootmise ja kasutamise kohana. „Praegu saab Vormsi elektrit merekaabli kaudu. Olukord rahuldab saare vajadusi, kuid me vaatame pikemalt tulevikku –

energia hind võib langeda ainult periooditi, aga üldine kasvutrend jõuab kriitilise piirini. Seetõttu otsime teisi lahendusi taastuvenergeetika valdkonnast,“ ütles Kongo.

Saare energiamajanduslikult sõltumatuks muutmine tähendaks päikese- või tuuleenergia kasutamist. Ühtlasi võimaldaks see igal majapidamisel olla ühtaegu nii tootja kui ka tarbija ning vajadusel saaks ülejääva osa energiat teistele edasi müüa.

Ehkki tuule- ja päikeseenergia tootmiseks vajalike seadmete maksumus on Kongo sõnul laias laastus sama, oleks saare jaoks parim lahendus kahe meetodi kombinatsioon. Otsustab Vormsi kogukonna soov.

„Keskendume rohkem päikesepaneelidele. Meie andmetel oleks märtsist kuni oktoobrini võimalik piisava arvu paneelide korral päikeseenergiaga saare elektrivajadus edukalt katta. Nutitelefoni rakenduse abil saaks iga tootja jälgida, kui palju tema paneel kindla ajavahemiku lõikes elektrienergiat tootis, kui palju sellest oma majapidamises ära tarbis ja saare üldvõrku müüs. Selline süsteem eeldab omakorda Targa Võrgu ehk Smart Gridi olemasolu,“ leidis juhatuse liige.

Kongo sõnul on projekti koordinaatoritel reaalseid mõõteandmeid päikese- ja tuuleenergia võimaluste kohta hetkel veel liiga vähe. Hea abimehena toetab Nutika Vormsi projekti Lääne-Eesti ettevõtja ja taastuenergia eestvedaja Tarmo Kadakas, kes on tuule- ja päikeseenergia tasuvuse mõõtmisega pikemalt tegelema.

2012. aasta märtsis sõlmis MTÜ Nutikas Vormsi koostöölepe Tallinna Tehnikaülikooliga. Ühisosa nähakse TTÜs arendatavate kaasaegsete tehnoloogiate kasutamisel Vormsi saare energiaühistu arendamiseks. Koostöölepe pakub üliõpilastele ka võimalusi potentsiaalseteks teadus- ja arendustegevusteks. Lisaks hakkab Tehnikaülikooli esindaja osalema MTÜ Nutikas Vormsi Nõuandva Koja töös, ühiselt plaanitakse osaleda ka rahvusvahelistes projektides.

Vormsit näevad huvitava taastuenergia lahenduste katsetamise kohana Eesti Energia ja jaotusvõrguna Imatra Elekter, lisaks on projektiga seotud Infotehnoloogia- ja Telekommunikatsiooni Liit ja mitmete teiste valdkondade ettevõtted.

Teenused muutuvad kättesaadavaks

Nutikas Vormsi aitab saare elanikele kättesaadavaks teha mitmed elutähtsad teenused ning arendada kohalikku majanduselu siseturismi edendamise näol.

„Meie arusaamade järgi toetub Hullo külakeskuse renoveerimine targa maja põhimõttele, kus võiks nutitelefoniga või arvuti kaudu juhtida kõiki igapäevaseid funktsioone eesotsas elektri- ja kütelahendustega ja kus hoone valgustus on lahendatud kaasaegsel LED-tehnoloogial. Tark maja ei pea tooma kaasa majanduslikku kasu, vaid toetama üldist tugisüsteemi,“ kirjeldas Kongo saare keskse objekti kontseptsiooni.

Nutikas Vormsi teeb tulevikus kohalike jaoks kättesaadavaks kaugmeditsiini – nii ei pea eriala- ja konsulteerimiseks sõitma teise Ees-

ti otsa. Samuti saavad kohalikud kooliõpilased laialdasemalt ära kasutada veebipõhise õppetöö võimalusi.

„Lisaks on saarele planeeritud kaugtöökohad. Ehkki kõik ettevõtted pole selleks päriselt valmis, on just IT-valdkond väga paindlik. Kui suvel perega Vormsile puhkama tulles avaneb võimalus töötajad HD kvaliteediga videokonferentside ning korraliku kontoripinna toel korda ajada, siis

Nutika Vormsi idee aluseks on viis aspekti: nutikad Vormsi inimesed, nutikas majandus, nutikas elukeskkond, mobiilsus ning saarel kättesaadavad avalikud teenused.

kujuneks sellest veenev argument suvituskoha valikul ja ühtlasi saaks puhkajad kauemaks paigale jääda. See omakorda tõstab nõudlust majutuskohtade, toitlustuspaikade ja meelelahutuse pakkujate järele ning kohalikud saavad pakkuda turismiteenuseid laiemas ulatuses. Taoline teravilakohendus edendaks kogu saare heaolu,“ tões Kongo.

Vormsi vald soovib tulevikus näha saare püsielanike arvu kasvamist ning selleks on plaan koostada elamumajanduskava. „Üritame välja selgitada, kuhu on Vormsil võimalik ja mõistlik kinnisvara arendada. Suur osa maast kuulub kunagiste omanike järeltulijatele, kes ise Eestis ei ela,“ selgitas juhatuse liige.

2012. aastal loodetakse Vormsil esimesed teetähised nutika tuleviku teel paika panna. „Alustame infrastruktuuride väljaehitamist ning Sviby sadama renoveerimist, mis võiks samuti nutikaid teenuseid juurde pakkuda,“ andis Kongo ülevaate esimestest eelseisvatest sammudest.

Tulevikus loodavad Nutika Vormsi eestvedajad oma kogemusi teistesse riikidesse viia – maailmas on vaid mõned saared, mis end targa energijahtimise toel ise majandavad – Bornholm ja Samsö Taanis ning Jeju Lõuna-Koreas.



E-veoseleht – metsandussektori asjaajamine paberilt elektroonseks



MÄRT RIDALA

mart.ridala@elion.ee
Elion Ettevõtted AS

E-veoselehe projekt on hea näide sellest, kuidas ettevõtete ja asutuste vahelise info liikumise korraldamiseks on võimalik juurutada ühtne IT-süsteem. Selliseid edulugusid on veel vähe, kuid sellistes süsteemides on tulevik!

Mis on e-veoseleht?

Metsamaterjali vedades on veokijuhil kohustus omada veoselehte, mis näitab, kes on koormas oleva puidu omanik, kes on selle vedaja ja kes saaja. Selle süsteemi eesmärk on puidu päritolu jälgitavus. Kuni 2011. aastani oli ainus võimalik veoseleht kolmes eksemplaris paberleht. 2011. aasta lõpus käivitatud e-veoseleht võimaldab aga kogu asjaajamise viia elektroonseks ja andmebaasipõhiseks.

Tänane seis

Augustiks 2012 on metsandussektori ettevõtted e-veoselehe süsteemi aktiivselt kasutusele võtnud. Sellega veetakse keskmiselt 8500 vedu kuus ning süsteemiga on liitunud üle 180 ettevõtte. Paljud suuremad ettevõtted, nagu RMK, StoraEnso, AS Lemeks, Horizon Pulp & Paper, on praktiliselt loobunud paberveosele-

hest. E-veoseleht on plaanis kasutusele võtta ka muu metsamaterjali, näiteks hakkepuidu veol. Ühe olulise täiendusena loodi teenusele 2012. aastal mobiilirakendus – nüüd saab asju ajada metsas otse veoautos.

E-veoselehe eelised

Tänu elektroonilisele infosüsteemile on olemas adekvaatne info. Nii puidu omanikul, vedajal kui ka saajal on võimalik jälgida, kuidas vedamine edeneb – nad saavad jooksvalt ülevaate olukorrast, ilma et peaksid veokijuhtidele helistama. Lisaks jooksvale infole on olemas ka statistiline ja ajalooline info. Näiteks on võimalik e-veoselehe süsteemis olevate andmete põhjal arvestada veotasude suurust või maksta metsaomanikule müüdüd puidu eest tasu.

Kas elektrooniline paber või kogu protsessi arendus?

Iga infosüsteemi loomisel tuleb esmalt vastata küsimusele, kas tahetakse lihtsalt viia praegune protsess arvutipõhiseks või ka seda parandada. Lihtsalt paberi asendamine elektroonilise kirjega on alati lihtsam, samas tõeline kasu tuleneb alles protsessi parandamisest. E-veoselehe puhul

otsustati projekti alguses kohe teha midagi enamat kui asendada paberleht arvutiga. Eesmärgiks seati ülevaatlikkuse suurendamine ja kõigi osapoolte töö efektiivsuse tõstmine. See otsus tegi küll projekti keerulisemaks, pikemaks ja kulukamaks, kuid tänu sellele on pärast süsteemi rakendamist sellest kasutajatele ka tunduvalt rohkem kasu.

Edu võti

Ettevõtetevahelist süsteemi on kordi raskem juurutada kui ettevõttesisest. See tähendab eri huvisid või tihti ka huvi puudust. Kui ettevõttesiseselt on paika pandud üks juht, kes otsustab, kas teha ja kuidas teha, siis mitme ettevõtte puhul on vaja jõuda konsensusse. Seega on selle projekti puhul eriti oluline Metsa- ja Puidutööstuse Liidu roll ning e-veoselehe projektirühm eesotsas StoraEnso Eesti logistikajuhi Mait Maraniga. Ainult tänu nende järjekindlale tööle oli võimalik kõik osapooled alates transpordiettevõtetest, metsaomanikest, saeveskite omanikest ja lõpetades politsei ja Keskkonnainspeksiooniga panna koostööd tegema.

Elioni roll projektis

Elioni roll oli antud projekti puhul teistsugune kui tavapärase IT-süsteemi majutusteenuse pakku-

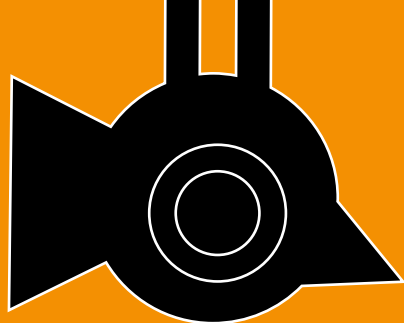
mine. Kui tavalise majutusteenuse puhul lepitakse teenuse saaja ja pakkuja vahel kokku konkreetsed süsteemi parameetrid ja majutuse hind, siis antud juhul pakub Elion e-veoselehe opereerimisteenust. See tähendab seda, et Elioni tasud tulevad e-veoselehe tasudest süsteemi kasutaja-

Iga infosüsteemi loomisel tuleb esmalt vastata küsimusele, kas tahetakse lihtsalt viia praegune protsess arvutipõhiseks või ka seda parandada. Lihtsalt paberi asendamine elektroonilise kirjega on alati lihtsam, samas tõeline kasu tuleneb alles protsessi parandamisest.

te käest ja lisaks majutusele on Elioni ülesandeks ka süsteemi arendamine, koolitamine, kasutajatuugi, infosüsteemide integreerimine ja klientide konsulteerimine. See on ka Elioni jaoks väga suur proovikivi, kuid tänaseks on selline teenus ennast igati õigustanud.







3. PEATÜKK

KÜBERTURVALISUS

Infotehnoloogia võimalusi kasutades peame üsna loomulikuks, et lisaks kõikidele muugavustele tuleb alati arvestada ka riskidega. Olgu selleks riskiks siis paljude inimeste elu mõjutavad küberrünnakud ettevõtete ja riigiasutuste vastu või lapsi ohustada võivad tegevused internetis. Küberturvalisuse valdkond muutub pidevalt ja järjest suurem sõltuvus infosüsteemidest seab nii riigisisese kui ka rahvusvahelise koostöö tähtsale kohale. Samas ei maksa kunagi unustada, et turvaline internet on ka iga ük-siku internetikasutaja teha. See peatükk annab ülevaate küberjulgeoleku strateegiast ning sellega seotud tegevustest, uuest infoturbe koosvõime raamistikust, küberturvalisuse tagamise organisatsioonilistest muudatustest, aga ka laste turvalisema internetikasutamise edendamise projektist „Targalt internetis“.



Küberjulgeolekust



HELENA RAUD

helena.raud@mkm.ee

Majandus- ja Kommunikatsiooniministeerium

Küberjulgeolek ja selle elemendid kinnistusid riigi retoorikasse peamiselt seoses 2007. aastal toimunud küberrünnakutega Eesti ettevõtete ja riigiasutuste veebilehtede ja teenuste vastu.

2008. aastal võttis valitsus vastu esimese küberjulgeoleku strateegia perioodiks 2008–2013. Kahtlemata oli see ajendatud ühest küljest 2007. aasta küberrünnakutest, kuid viis aastat tagasi oli Eesti infoühiskond ja sõltuvus tehnoloogiast ka juba niivõrd arenenud, et riigi rolli ei saanud turvalisema e-ühiskonna loomisel kuidagi eirata.

Küberjulgeoleku strateegia seadis riigile neli eesmärki.

1. Eestis on laialt rakendatud astmeline turvameetmete süsteem, mis tagab riigi küberjulgeoleku.
2. Eesti on väga suure infoturbealase kompetentsuse ja teadlikkusega riik.
3. Infosüsteemide turvalist ja laialdast kasutamist toetab proportsionaalne õiguslik regulatsioon.
4. Eesti on küberjulgeoleku tõhustamiseks tehtava rahvusvahelise koostöö üks juhtriike.

2012. aastal sai nendest märgilistest rünnakutest viis aastat – on aeg seatud eesmärgid üle vaadata, analüüsida tehtut ja seada uued sihid. Kuna uue perioodi strateegia koostamine on alles algusjärgus, siis annan esmalt põgusa ülevaate nendest valdkondadest, millega oleme küberjulgeoleku kontekstis tegelenud.

Infosüsteemide turvalisus – valitsuse määrus „Infosüsteemide turvameetmete süsteem“ võeti

vastu juba 20.12.2007 ning sellega loodi alus turvameetmete süsteemi rakendamisele riigiasutustes. Selleks et tagada veelgi paremat koordineerimist ja intsidentidest raporteerimist, kehtestas valitsus 2012. aastal määruse „Infoturbe juhtimise süsteem“, mis tegi riigiasutustele kohustuseks määrata ametisse infoturbejuhid. Vastavalt määrusele teeb infoturbejuht oma ülesannete täitmisel koostööd isikuandmete töötlemise eest vastutava inimesega, kontrollib infoturvet reguleerivate juhiste täitmist, hindab asutuse infoturbe tõhusust ning koostab selle kohta raporti, osaleb asutuse arendus- või IT-nõukogu töös ja infosüsteemide arendusprojektides, nõustab infoturbe riskide hindamisel, uute turvameetmete loomisel või olemasolevate parandamisel, juurutab asutuses turvaintsidentide haldamise korra ning teavitab CERT-EED olulistest turvaintsidentidest.

Küberohte arvestava õigusliku raamistiku korramisega on samuti tegeldud aktiivselt alates strateegia perioodi algusest. Sinna jääb nii karistusseadustiku muutmine ning hädaolukorra seaduse muutmine kui ka 2012. aastal vastu võetud Kaitseliidu seaduse muudatus, mis annab aluse Kaitseliidu küberkaitseüksuse tegevusele.

Õppused – nende roll küberjulgeoleku regulatsioonide testimisel on märkimisväärne, sest mittetoimiv seadusandlus või puudulikud otsustusmehhanismid võivad oluliselt mõjutada küberohtudest tulenevate kriiside lahendamist kõigis elutähtsate teenuste sektorites.

2012. aasta jaanuaris toimus Eestis veel ainulaadne küberõppus „Küberpalavik 2012“, mille

stsenaariumi ja korralduse tagas Kaitsejõude küberkaitseüksus. Kui asutused ja organisatsioonid on ikka tehnilisi küberõppusi korraldanud, siis „Küberpalavik 2012“ oli esimene õppus valitsusele ja selle kriisikomisjonile.

Rahvusvahelised ülesanded – mõistagi on internetiseerunud ja piirideta maailmas oluline küberriskide ühtsete põhimõtete, arusaamade väljatöötamine ja tõhus riskide maandamine. Eesti on olnud aktiivne nii kahe- kui ka mitmepoolses koostöös, kuid kahtlemata on meie suurim panus olnud rahvusvahelistes organisatsioonides, nagu EL, NATO ja OECD.

MKMi ja RIA esindajad osalesid 2011. aastal aktiivselt esimese ENISA koordineerimisel korraldatud EL-USA küberõppuse „Cyber Atlantic“ planeerimisel ja läbimängimisel. Eesmärgiks oli lisaks tehniliste lahenduste kaardistamisele tutvustada kõigi ELi liikmesriikide ja USA ning ELi institutsioonide küberexperte nii tehnilisel kui ka poliitika planeerijate tasemel.

2012. aastal oleme samuti tihedalt seotud hilisügisel Ateenas toimuva ELi õppuse „Cyber Europe“ planeerimisega. Väikeriigina, kes on võtnud endale kohustuse hoida kõrget taset küberjulgeoleku tagamisel, oleme rõõmsad, et õppuse avasõnad peakoordinaatori ENISA ja MKMi esindajatelt kostavad just Tallinnast.

Lisaks õppustele on 2012. aasta ELis märgiline seoses laiapõhjalise üleeuroopalise küberstrateegia koostamise algatamisega.

Organisatsioonilistest muudatustest uue strateegiani – 2011. aastal leidis aset suurim organisatsiooniline muudatus küberjulgeoleku korraldamisel. Nimelt andis Kaitseministeerium 2010. aasta lõpus küberjulgeoleku strateegia koordineerimise ja küberjulgeoleku nõukogu juhtimise üle Majandus- ja Kommunikatsiooniministeeriumile. Kuivõrd paljudes meie partnerriikides

koordineerib riigiülest küberjulgeolekut just kaitseministeerium, siis võiks küsida, miks selline muudatus tehti.

Me võime vastata praktilisest ja kommunikatsioonivaldkonda puudutavast aspektist: seda tingis asjaolu, et küberohud ja kommunikatsiooni infrastruktuur, mida kasutavad nii tavakodanikud kui ka riik, on valdavalt eraettevõtete tagada. Kommunikatsiooniteenuste toimepidevuse reguleerimine on jällegi MKMi haldusala. Kuid samavõrd oluline on MKMi roll teiste elutähtsate

Eesti on olnud aktiivne nii kahe- kui mitmepoolses koostöös, kuid kahtlemata on meie suurim panus olnud rahvusvahelistes organisatsioonides, nagu EL, NATO ja OECD.

teenuste toimepidevuse tagamise korraldamisel (näiteks energeetika sektoris) või asjaolu, et samasse haldusalasse kuulub 2011. aastal ümber korraldatud Riigi Infosüsteemi Amet (RIA) ja selle koosseisus asuv CERT.

Tulevikuplaanide kohta võime öelda, et suurimaks ülesandeks on 2012. aastal algatav ja 2013. aasta jooksul koostatav teine küberjulgeoleku strateegia ning küberjulgeolekut puudutava õigusliku raamistiku korrastamine.

Esmakordselt hakkab strateegia koostamise koordineerimise eest vastutama MKM, kuid äärmiselt oluline roll on ka meie partneritel teistest ministeeriumidest, riigiasutustest, erasektorist ja ka akadeemilistest ringkondadest. Kuigi praegu on veel vara rääkida uutest strateegilistest eesmärkidest, loodame ja töötame siiski selle nimel, et Eesti teine küberjulgeoleku strateegia oleks veel laiapindsem ja arvestaks võimalikke küberohte meie infoühiskonna arenguga kooskõlas, seadmata liigseid piiranguid.



Riigi Infosüsteemi Ameti roll Eesti küberturvalisuse tagamisel



TOOMAS VAKS

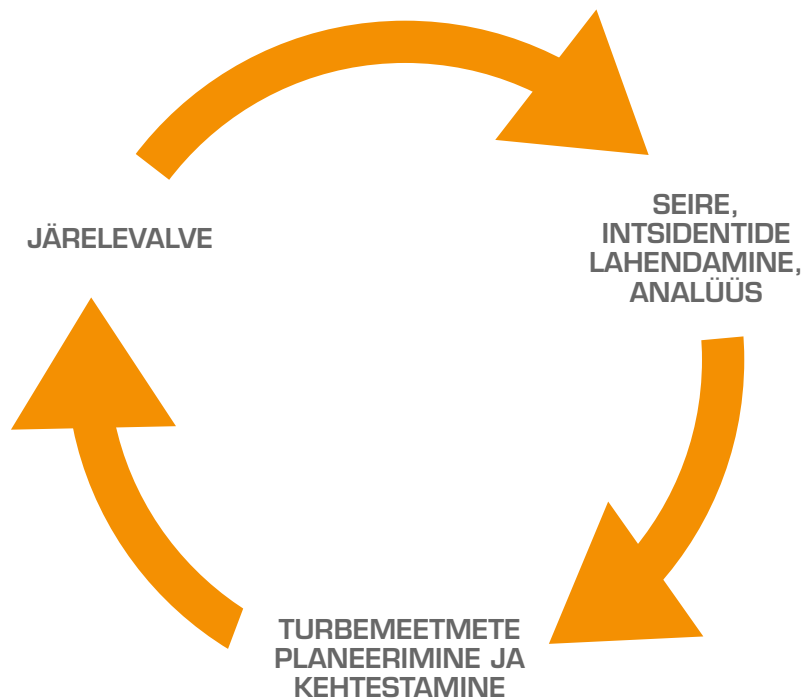
toomas.vaks@ria.ee
Riigi Infosüsteemi Amet

Alates 2000. aastate algusest on Eesti riigi areng olnud tihedalt seotud infotehnoloogia arenguga. Riigina, kus on vähe elanikke ja mille asustustihedus on üks väiksemaid Euroopas, on panustamine infotehnoloogia ja kommunikatsioonivaldkonna arengusse olnud loogiline ja paratamatu samm. Ilma tänapäevase infotehnoloogiata oleksid paljud meile praegusel ajal harjumuseks saanud avalikud ja ka erasektori teenused vajaliku inimressurssi puudumise tõttu kas võimatud või väga kallid. Siinkohal võib näiteks tuua sellised infomahukad teenused nagu riiklikud ja eraregistrid, infobaasid, meedia, pangandus jne.

Eesti oludes on väga oluline ka teenuste kättesaadavus väljaspool suuri keskuseid, mis võimaldab paljude vajalike toimingute tegemist ka hõreasustusega paikades. Viimaste aastate jooksul on sõltuvus infosüsteemidest kasvanud ka valdkondades, mis pole otseselt seotud infotöötusega. Tööstusseadmete juhtimissüsteemid (ICS ja SCADA) on tänapäeval järjest rohkem integreeritud internetiga ühendatud süsteemidega ning veebi kaudu juhitavad seadmed on tunginud ka meie igapäevasesse ellu. Kaugjuhitavad ja -jälgitavad kütteseadmed, varugeneraatorid, signalisatsioon- ja valveseadmed on vaid mõned sellised näited. Seega on paratamatult üles kerkinud ka riskide teema. Eriti aktuaalseks muutusid need diskus-

sioonid pärast küberkuritegevuse hoogustumist 2000. aastate algupoolel ning loomulikult avasid neis arutlustes täiesti uue lehekülje 2007. aastal toimunud küberrünnakud. Küsimused, mis puudutavad sõltuvust riigi ja ühiskonna infosüsteemidest ja sellega seotud riskidest, tingisid ka vajaduse senisest terviklikuma ning efektiivsema lähenemise järele taoliste riskide ohjamisel ja nii loodigi infosüsteemide arenduskeskuse baasil 1. juunist 2011 Majandus- ja Kommunikatsiooniministeeriumi valitsusalas uue valitsusasutusena Riigi Infosüsteemi Amet (RIA), mille üks peamisi ülesandeid ongi küberturvalisuse tagamine Eestis. RIA ülesanneteks on selles valdkonnas järelevalve teostamine elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete alalise rakendamise üle, riigi infosüsteemi ja Eesti kriitilise informatsiooni infrastruktuuri infoturbe seotud tegevuste korraldamine, Eesti arvutivõrkudes toimuvate turvaintsidentide käsitlemine ja loomulikult ka osalemine oma tegevusvaldkonnaga seotud poliitikate, strateegiate ja arengukavade väljatöötamisel.

Küberturvalisusega tegelevad kolm RIA osakonda: kriitilise info infrastruktuuri kaitse osakond (KIIK), infoturbeintsidentide käsitlemise osakond (CERT-EE) ning järelevalve osakond (JVO) – nen-



Peamised küberturvalisuse tagamiseks kasutatavad riiklikud vahendid.

de tegevust koordineerib peadirektori asetäitja küberturvalisuse valdkonnas. Peamised tegevussuunad on:

- kriitilise informatsiooni infrastruktuuri kaitse korraldamine, sh riskianalüüside koostamine ja kriitilise informatsiooni infrastruktuuri kaitseks vajalike turvameetmete arendamine;
- infoturbe standardite (sh infosüsteemide kolmeastmelise etalonturbe süsteemi ISKE) rakendamise koordineerimine riigi ja kohaliku omavalitsuse asutustes ja avalikke ülesandeid täitvate eraõiguslike isikute juures ning infoturbealaste soovitude väljatöötamine selleks;
- Eesti arvutivõrkudes toimuvate ja ametile raporteeritud turvaintsidentide käsitlemine, hoiatuste edastamine turvaintsidentide ennetamiseks ning kasutajate turvateadlikkuse tõstmise, sh ka raportite koostamine Eesti arvutivõrkudes toimunud intsidentidest ja pahavara leviku kohta;
- küberturbega seotud strateegiate ja poliitika arendamine;
- järelevalve elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete alalise rakendamise üle;
- koostöö teiste valitsusasutuste, kohaliku omavalitsuse üksuste, sihtasutuste, mittetu-

lundusühingute, ettevõtlus- ja tarbijaorganisatsioonidega ning teiste vastavate asutuste ja rahvusvaheliste organisatsioonidega, samuti riigiasutuste nõustamine valdkonna probleemide lahendamisel;

- riigi esindamine rahvusvahelisel suhtlemisel õigusaktidega ettenähtud korras.

RIA ei pidanud küberturbe tagamisel alustama aga tühjalt kohalt. Juba 2006. aastast tegutsenud infoturbeintsidentide lahendamise üksus CERT-EE ning paar aastat hiljem infosüsteemide arenduskeskuse koosseisus loodud kriitilise info infrastruktuuri kaitse osakond olid selleks väga hea vundamendi loonud. Nende üksuste spetsialistid on oma ala rahvusvaheliselt tunnustatud professionaalid, kelle teadmised ja initsiatiiv on võimaldanud säilitada küberjulgeoleku valdkonna rahuldav võimekus ka majanduslanguse tingimustes. Eestis on õnnestunud luua väga hea koostöö era- ja riigisektori vahel, mis on loonud välisriikide jaoks küllaltki omapärase *security community*, kes vahetab igapäevaselt operatiivset infot küberjulgeoleku valdkonnas toimuvate intsidentide ning turvariskide kohta.

Riigiasutuste, elutähtsaid teenuseid osutavate ettevõtete ja asutuste töötajate ning ka elanik-»

» konna turvateadlikkuse tõstmine on olnud üks küberturvalisuse valdkonna peamisi riiklikke prioriteete. 2011. aastal korraldati ELi programmi „Infoühiskonna teadlikkuse tõstmine“ raames toimivas koolitustesarjas „Tark e-riik“ 32 küberturvalisuse teemalist koolitusüritust, millest võttis osa kokku 966 inimest. Väga heaks tuleb lugeda ka rahvusvahelist koostööd, mis on tänu suurepärasele infovahetusele ära hoidnud ja tõkestanud turvaintsidente ning tõhustanud kaitsemeetmeid.

2011. aasta jooksul õnnestus muuhulgas uuendada kolmeastmelist etalon turbe süsteemi (IS-KEt) ja viia lõpule mitmeid riskianalüüsi riigile olulistest valdkondades.

Pärast RIA moodustamist algas ka täiendavate küberturvalisuse spetsialistide otsing, et mehitada järelvalve osakond ning leida lisatöajõudu ka CERTi ning KIIKi osakondadesse. Heameel on tõdeda, et hoolimata Eesti ja ka rahvusvahelisel tööjõuturul valitsevast suurest nõudlusest küberturbe spetsialistide järele, on nii mõnigi rahvusvaheliselt tunnustatud spetsialist asunud tööle riigiametisse ning ühinenud RIA meeskonnaga. Praegu on 19 RIA töötaja ja ametniku igapäevane töö seotud just küberturvalisuse kindlustamisega.

2011. aasta märksõnadeks olid meile küberjulgeoleku valdkonnas järgmised.

- E-faktor – küberturvalisuse tagamine on Eestis paratamatu, kuna paljud riigi ja erasektori teenused sõltuvad täielikult infotehnoloogilistest vahenditest.

- Rahvusvaheline koostöö küberturvalisuse valas on väga intensiivne ja alanud on ka rahvusvaheliste regulatsioonide väljatöötamine ning kehtestamine.
- Hädaolukorra seaduse parandusettepanek ehk nn serverite eelnõu algatas ühiskonnas diskussiooni elutähtsate teenuste infotehnoloogiliste sõltuvuste üle.
- Mobiilseadmed ja sotsiaalmeedia on muutnud inimeste käitumist ja turvariske.
- ICS/SCADA-süsteemide riskid on toonud turvariskid infoturbest igapäevaellu.
- Järelevalve sisseseadmine elutähtsa teenuse infosüsteemide turvameetmete rakendamise üle.

2012. aastal näemegi suurimate ülesannetena küberturbe riskide seire ja analüüsi tagamist, nende asjakohast ja õigeaegset teavitust ning vastumeetmete rakendamist. Samuti vajab veel enam tähelepanu intsidentide lahendamise ja ärahoidmise sisulise võimekuse säilitamine-arendamine ja efektiivne rahvusvaheline koostöö.

Kokkuvõttes tuleb tõdeda, et infosüsteemidega seotud riske pole võimalik välistada, kuid neid on võimalik kontrollida ning seeläbi ka vähendada kahjusid. Riskide ohjeldamiseks on vaja neist aru saada ning õigesti hinnata ohtu, selle mõju ja saabumise tõenäosust. Suurimaks ohuks küberjulgeoleku valdkonnas on endiselt ikkagi tehnoloogia kasutaja oskamatus, lohakus või hoolimatus ning suutmatus hoomata tehnoloogia arengut ja sellega seotud riske.



Eesti turvalisemat üleilmset küberruumi ehitamas



LUUKAS KRISTJAN ILVES

luukas.ilves@ria.ee
Riigi Infosüsteemi Amet

Olukord maailmas

Rahvusvahelise koostöö vajadus küberruumis on ilmselge. Küberruum on üleilmne ja ükski riik ei ole kübersaar, ent praegu on küberjulgeolek samal arengutasemel kui merejulgeolek 18. sajandil: pahad tegutsevad piiriüleselt ja karistamatult, valitsusväliste ja riiklike toimijate vahel on raske vahet teha, ründajail on kaitsjate suhtes eelised ning küberrünnakute asümmeetrilised kulud ja tulud soosivad kõik ebakindluse kasvu.

2011. aastal ei saanud maailm enam küberohete ja kaitsetust eirata. Mis toimus? Wikileaks kaudu dokumentide aeglane ja pidev lekitamine, teabe mahavaikimine valitsuste poolt ja *Anonymouse*-taoliste häkker-aktivistide kättemaks Wikileaksile vaikimasundimise katse eest, Araabia kevad, mis näitas sotsiaalmeedia kui organiseerimisvahendi võimsust valitsuste kukutamisel, lakkamatu jutt paroolide ja krediitkaardiandmete vargustest, laia kõlapinda leidnud küberkuritegevuslike rühmituste vahistamine (Rove Digital Eestis), ulatuslikud andmekaitsealased rikkumised ELis, IMFis ja ÜROs ja paljudes kaitseministeeriumides ja ettevõtetes ning Stuxneti pahavara veelgi võimsam järglane Duqu.

Paljud riigid on ka ohule reageerinud. Mitmed neist, näiteks Saksamaa, Ühendkuningriik ja USA, avalikustasid oma riikliku küberjulgeoleku strateegia. NATO võttis uue küberkaitsepoliitika vastu 2011. aasta juunis. EL ja USA kooskõlas-

tavad poliitikat mitmes töörühmas. Euroopa Julgeoleku- ja Koostööorganisatsioon (OSCE) töötab välja küberusalduse suurendamise ja küberjulgeoleku tugevdamise meetmeid. 2011. aastale pani punkti suur rahvusvaheline konverents Londonis, mille eesmärk oli töötada välja ühised normid küberruumi kohta ja mille jätk toimub sellel aastal Budapestis. ÜRO alustab järgmist arutelude vooru, et jõuda küberruumis käitumise normide asjus rahvusvahelisele kokkuleppele – Eesti on nende 15 riigi seas, kes osalevad ÜRO riiklike ekspertide rühmas. Eesti on olnud kõikidel foorumitel väga aktiivne osaleja ja kuulunud nende väheste riikide sekka, kes kujundavad poliitilist konsensust.

Arutelude sisu siiski muutub, sest läbirääkimised rahvusvahelistes organisatsioonides ja partneritega on läinud tehnilisemaks ning mitmepoolse ja kahepoolse küberkoostöö sügavus ja ulatus on suurenenud. Seni on Eesti suutnud hoida selles vallas oma poliitilist ja juhtpositsiooni, ent selle säilitamine on väikesele riigile, mille avalik sektor on veelgi väiksem, raske ülesanne.

Eesti strateegilised eesmärgid

Eesti põhilised töekspidamised rahvusvahelise küberjulgeolekuga tegelemisel ei erine seisukohtadest, mis sõnastati 2008. aastal riiklikus küberjulgeoleku strateegias.

- Lähtuda laiast lähenemisviisist sidusrühmadele, kaasates valitsused, erasektori, kodani-»

- » kuühiskonna, rahvusvahelised organisatsioonid, eksperdid. Vestfaali suveräänsussüsteemi reegleid pole võimalik lihtsalt internetile laiendada.
- Töötada välja õigus- ja käitumisnormid riigi käitumiseks küberruumis, sh sõjaõigusest tulenevad normid, ja neid levitada.
- Võtmetegevuseks on võitlus küberkuritegevuse vastu, mis aitab vähendada riikidevahelisi küberkonflikte. Küberkuritegevus on juba iseenesest hirmuäratav nähtus, ent see võimaldab ka riikide toetusel toimival spioneerimisel ja rünnakutel jääda nn hallile alale, saamata rahvusvahelise üldsuse selget heakskiitu ega ka hukkamõistu.
- Jääda kindlaks liberaalsetele ja kaasavatele tavadele, mis on seni interneti haldamist iseloomustanud, tagades, et veeb jääb vabaduse teostamise vahendiks ja seda ei turvata üleliia.

Küberjulgeoleku vallas ei kannata Eesti üleilmse nähtavuse puudumise all. Eesti on olnud alates 2007. aasta rünnakutest üleilmne liider ja riigil on olemas järjepidev rahvusvaheline poliitika ja tehniline tegevuskava.

Tegelikult on Eesti rõhutanud nii oma tegevuses kui ka kõikides suhetes avatust, läbipaistvust, teabe jagamist ja koostööaldist lähenemisviisi. Väikese riigina saab Eesti oma küberjulgeoleku saavutada üksnes koostöös teistega.

Eesti rahvusvahelise tegevuse koordineerimine on keeruline ülesanne. Isegi meie väikesel riigil on pikk nimekiri osalistest, kes vastutavad küberjulgeoleku eest ja tegutsevad rahvusvaheliselt. Poliitika tasandil on juhtohjad Majandus- ja Kommunikatsiooniministeeriumi käes, kuid osaliste seas on ka Riigikantselei ja Presidendi Kantselei, Kaitse-, Sise-, Välis- ja Justiitsministeerium. Operatiivtasandil on osalised Riigi Infosüsteemi Amet, kaitsejõud ja mitmesugused politseiasutused.

Tehniline koostöö

Ainuüksi rahvusvahelistest konverentsidest ning NATO ja ELi strateegiatest ei piisa selleks, et kaitsta end välismaise küberrünnaku eest. Rah-

vusvaheline koostöö küberruumi vallas peab arendama tõhusamat operatiivvõimekust. Eesti-suurusel riigil on eriti vaja toetuda ELi ja NATO tegutsemisvõimekusele. Kuigi mitteametlik koostöö Eesti ja samamoodi mõtleivate riikide vahel on olnud suurepärase, on siiski olnud raske seda formaliseerida.

Hea näide keskendumisest tehnilisele koostööle, mis on andnud selgeid tulemusi, on Eesti, Soome ja Belgia CERTe hõlmav ühisprojekt Abusehelper, mis töötleb automaatselt intsidentide teateid ning aitab riikidel vähendada pahavaraga nakatumise määra ja robotvõrgustike arvu oma domeenis.

NBS ja kahepoolne koostöö

Suurem piirkondlik lõimumine ei ole valikuvõimalus, vaid vajadus. Eestil on küberjulgeoleku alal kõige tihedamad kontaktid oma naabrite Läti ja Leeduga (kolm Balti riiki) ning Soome, Rootsi, Taani, Norra ja Islandiga (viis Põhjamaad). Need riigid sõltuvad küberruumis üksteisest väga, sest pangandus-, telekommunikatsiooni- ja energiasektor on üha rohkem omavahel ühendatud, seda ka füüsilises mõttes (elektrikaablite ja kiudoptiliste kaablite kaudu). Ulatuslik küberrünnak ühe riigi elutähtsate teenuste vastu tekitaks kahju kõikide riikide kodanikele ja ettevõtetele.

NBS-I (viiel Põhjamaal ja kolmel Baltimaal) on sarnane küberohtude hindamise ja riigisiseste meetmete kogum, peatähelepanu pööratakse olulise tähtsusega taristu kaitsmisele ja vahendeid on ühtviisi napilt. Kõikides riikides on riigisisese küberruumis pahavaraga nakatumise ja kuritegevuse tase madal. Nende maade tehniline koostöö on juba tihe ning Eesti lõppeesmärk on saavutada ühtlaselt kõrge küberjulgeoleku tase, mis võimaldaks ühendada nende tegevuse selles valdkonnas.

Eesti teeb tihedat koostööd paljude teiste partneritega. Eesti valitsussektori IT-turvalisuse suunised (ISKE) põhinevad Saksamaa Liitvabariigi IT-turbe standardil (*IT Baseline Protection Manual*). Eesti ja USA ametiasutused teevad tihedat koostööd küberkuritegevusega võitlemisel, viimati rämpsposti ja reklaamvara levitava ettevõtte Rove Digital laia kõlapinda leidnud likvideerimisel 2011. aasta novembris, mille näol oli tegemist

seni maailma suurima küberjulgeolekuga seotud vahistamise ja süüdistuse esitamisega. Mitu Eesti valitsusasutust, nende seas infosüsteemi amet, teevad võimekuse suurendamise ja koolituse vallas koostööd välispartneritega, eriti Kaagu-Euroopast ning üha enam ka Lähis-Idast ja Põhja-Aafrikast.

Rahvusvahelised institutsioonid

Lisaks riiklikele eriteadmistele kasutab ja toetab Eesti Tallinnas tegutsevaid rahvusvahelisi institutsioone. NATO kooperatiivse küberkaitse kompetentsikeskuses (CCD CoE) töötab palju eestlasi ning keskus teeb ühiste programmide ja õppuste raames koostööd kaitsejõudude ja Eesti Küberkaitse Liiduga. ELi Schengeni IT-agentuuri käivitamine 2012. aastal suurendab veelgi Tallinnas elavate rahvusvaheliste ekspertide arvu.

Õppused

Eesti osaleb väga aktiivselt rahvusvahelistel küberjulgeoleku õppustel. Eesti roll ELi ja NATO õppuste, näiteks „Cyber Europe'i“ ja „Cyber Coalitioni“ kavandamisel on olnud väga suur ja koos küberkaitse kompetentsikeskusega korraldatakse piirkondlikke õppusi, nagu „Locked Shield“, samuti kutsuvad Eesti välisvaatlejaid oma tehnilistele ja teoreetilistele õppustele. Hiljutiste õppuste seas oli „Küberpalavik 2012“, kahepäevane valitsuse tasandil staabiõppus, mille korraldas Kaitseliidu küberkaitse üksus.

Hallid pilved silmapiiril

Paraku on silmapiiril näha ka halle pilvi. Üks muret tekitav rahvusvaheline suundumus on küber-

julgeoleku suurenev julgeolekustamine. CERTide rahvusvaheline võrgustik, mis kasvas 1990. aastatel välja akadeemilisest maailmast, oli paindlik, tsentraliseerimata ja väga avatud, sellel puudusid ametlikud kokkulepped teabe jagamiseks. Ent kuna küberjulgeolekust on saanud suurema tähtsusega riiklik küsimus, käsitlevad riigid seda sõjalise ja luureteemana ning suunavad oma võimekuse arendamise organisatsioonidesse ja õigusstruktuuri, mis raskendavad rahvusvahelist koostööd, selle asemel et seda soodustada. NATO ja EL ei ole saavutanud koostöö ja ühise tegutsemisvõime samasugust taset nagu kaitsealase, õiguskaitsealase või terrorismivastase koostöö vallas. Paljud NATO liitlased ja ELi liikmesriigid lihtsalt ei taha usaldada nii olulise probleemi lahendamist rahvusvahelistele organisatsioonidele.

Olukorra teeb veelgi keerulisemaks küberjulgeoleku temaatika suhteline uudsus, mille tõttu on töö jaotatud igas riigis eri moel Kaitse-, Sise- ja Majandusministeeriumi ning CERTide, õiguskaitse-, luureasutuste ja sõjaväe vahel. Kõik see teeb rahvusvahelise koostöö kohati segaseks ja raskeks.

Küberjulgeoleku vallas ei kannata Eesti üleilmse nähtavuse puudumise all. Eesti on olnud alates 2007. aasta rünnakutest üleilmne liider ja riigil on olemas järjepidev rahvusvaheline poliitika ja tehniline tegevuskava. Kasvava globaalse küberjulgeolekule osutatud tähelepanu (ja konkurentsi) tingimustes peame nüüd aga rohkem pingutama. Surve ja ootused Eesti valitsusele, poliitika kujundajatele, ametiasutustele ja tehnilistele ekspertidele ei vähene.



Infoturbe koosvõime raamistiku ver 2



JAAK TEPANDI

jaak@tepandi.ee
Tallinna Tehnikaülikool

Piirid reaalse ja virtuaalse vahel on hägustunud. Meie heaolu, vara ja elu ei määra mitte ainult füüsilise, vaid ka kübermaailma reeglid. Viimased on aga alles kujunemisel. Infoturbe koosvõime raamistik on üks regulatsioonidest, mis püüab kujundada turvalist küberkeskkonda.

Raamistikust on alates 2007. aastast ilmunud neli ametlikku versiooni. Neist viimane on versioon 2 (www.riso.ee/et/koosvoime/infoturberaamistik-2011.odt), mis arvestab vahepealseid muudatusi Eestis, Euroopa Liidus ja kogu maa-

Piirid reaalse ja virtuaalse vahel on hägustunud. Meie heaolu, vara ja elu ei määra mitte ainult füüsilise, vaid ka kübermaailma reeglid.

ilmis, eelkõige kriitilise informatsiooni taristu kaitse olulisust ning uute tehnoloogiate (nt mobiilsete sidevahendite ja intelligentsete seadmete võrgud) kasutuselevõtuga seotud turvariske.

Nagu füüsilise maailma puhul, tuleb ka küberkeskkonna kaitseks rakendada mitmeid regulatsioone. Nii on infoturbe koosvõime raamistik ning „Küberjulgeoleku strateegia 2008–2013“ omavahel kooskõlas ja seotud, kuid neil on erinevad sihtgrupid, orientatsioon ja sisu. Küberjulgeoleku mõiste hõlmab kõiki elektroonilise teabe, teabekandjate ja -teenustega seotud toiminguid,

mis mõjutavad riigi julgeolekut. Küberjulgeoleku strateegia on suunatud eelkõige (kuigi mitte ainult) riigikaitse ja kriitilise informatsiooni taristu kaitsega seotud asutustele. See tugineb eeskätt riigi kui terviku küberruumi haavatavuse vähendamisele, keskendub riigi julgeolekule ning hõlmab mitmeid riigisaladusega seotud valdkondi.

Infoturbe koosvõime raamistik määrab kindlaks Eesti infoturbe toimimise üldpõhimõtted. See on mõeldud riigiasutuste ja erasektori ühtsete standardite kehtestamiseks riigisisese infoturbe tagamisel, sealhulgas avalike teenuste pakkumiseks kasutatavate infotehnoloogiliste lahenduste arendamisel ja haldamisel. Raamistik ei käsitle riigisaladusega seonduvat.

Infoturbe raamistiku versioon 2 käsitleb eelmistest põhjalikumalt kriitilise informatsiooni taristu kaitset. Sealjuures on lähtutud e-ühiskonna ja avaliku sektori seisukohast, täpsemalt sellest, mida asutused ja ettevõtted peavad arvestama seoses kriitilise informatsiooni taristu kaitsega ning millised on infosüsteemi koosvõime küberjulgeoleku aspektid.

Kriitilised taristud koosnevad sellistest füüsilistest ja infotehnoloogia rajatistest, võrkudest, teenustest ja ressurssidest, mille häirimine või hävitamine mõjutab tugevalt kodanike tervist, ohutust, julgeolekut, majanduslikku heaolu või valitsuste toimimist. Kriitilised taristud hõlmavad

paljusid majandussektoreid, kaasa arvatud pangandus ja rahandus, transport ja turustamine, energia, kommunaalmajandus, tervishoid, toiduga varustamine ja side ning valitsuse võtmeteenistused.

Siseministri määruses „Toimepidevuse riskianalüüsi koostamise juhend“ on nimetatud elutähtsad teenused. Need on teenused, mis on hädavajalikud eluliselt tähtsate ühiskondlike toimingute, tervishoiu, turvalisuse, julgeoleku ning inimeste majandusliku ja sotsiaalse heaolu korraldamiseks. Hädalukorra seaduses sätestatakse, et elutähtsa teenuse osutaja „on kohustatud tagama nende osutamiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete alalise rakendamise“.

ISKE rakendamise käigus võib infosüsteemidega seotud elutähtsaid teenuseid analüüsides selguda riigi ja kohaliku omavalitsuse andmekogu täiendavate turvanõuete vajadus.

Teiste andmekasutajate vajaduste arvestamisel tuleks erilist tähelepanu pöörata võimalikele seostele kriitilise taristuga (nt selle varade, teenuste või süsteemidega). Kui sellised seosed on olemas, tuleks neid arvestada süsteemide turvaklasside, -astmete ja -meetmete valikul.

Kriitilise informatsiooni taristu teenused on tihti sõltuvusahelates. Näiteks mõne elutähtsa teenuse toimimiseks on vaja tervet rida komponentsüsteeme ja -teenuseid. Kui asutus või ettevõtte on üks komponent sellises ahelas, tuleks seda kindlasti arvestada. Täiendavaid turvanõudeid tuleks kaaluda ka juhul, kui organisatsiooni süsteemid võivad mõjutada interneti taristu toimimist või on seotud SCADA juhtimissüsteemidega.

Täiendavaid turvanõudeid tuleks arvestada ka allhankelepingutes, sealhulgas teenusepakujate serveriruumide ja muu taristu osas.



Koostöö laste turvalisema internetikasutuse edendamiseks



KERLI KUUSK

kerli@lastekaitseliit.ee
MTÜ Lastekaitse Liit

Lapsed ja noored on aktiivsed uute meediatehnoloogiate kasutajad, saades nii osa uutest võimalustest, mida pakuvad interneti suhtluskeskkonnad, *online*-mängud, mobiilside jne. Kuid oluline on, et neil oleks sealjuures teadmised, kuidas neid tehnoloogiaid ilma ennast ega teisi ohtu seadmata kasutada ning kust vajadusel abi ja nõu saada. **Turvalisema internetikasutuse edendamiseks Eestis algatati Lastekaitse Liidu koordineerimisel 2010. aasta septembris projekt „Targalt internetis“**, mida viivad ellu MTÜ Lastekaitse Liit, Politsei- ja Piirivalveamet, Tiigrihüppe Sihtasutus, Sotsiaalministeerium ja MTÜ Abikeskused. Projekti eesmärgiks on laste ja lastevanemate targem internetikasutus ning ebaseadusliku sisuga materjalide leviku tõkestamine. Projektis on kolm tegevussuunda: koolitus- ja teavitustöö, ebaseadusliku sisuga materjali leviku tõkestamine veebipõhise vihjeliini www.vihjeliin.ee tegevuse raames ja nõustamine lasteabitelefonil 11 6111. Siin on ülevaade projekti tegevustest ajavahemikul jaanuar 2011 kuni mai 2012, laste turvalisema internetikasutuse edendamiseks koostatud materjalidest ning sellest, kust neid leida.

Koolitus- ja teavitustöö

Koolitus- ja teavitustööd koordineerib Tiigrihüppe Sihtasutus, kelle eestvedamisel kor-

raldati lastele, lastevanematele ja õpetajatele mitmeid koolitus- ja teavitussuureid. 2011. aasta algul alustati laiaulatusliku koolitustegevusega koolides ja ka lasteaedades üle Eesti. 15 koolitajat, kes korraldavad loenguid ja õpitubasid nii eesti kui ka vene keeles, andsid interneti turvalisusest teadmisi 9194 õpilasele, 1176 lapsevanemale ja 1157 õpetajale, külastades kokku üle 150 kooli ja lasteaia. Koolituse info ja koolitajate kontaktid on saadaval veebilehel www.targaltinternetis.ee. Töötubade kaudu saavad õpetajad julgustust ja teavet, kuidas antud teematikat oma tundides õpilastele edasi anda. Lisaks koolides toimuvatele teavitussuurete korraldati õpetajatele neli internetiturvalisuse e-kursust, kus käsitleti arvutikaitse, sotsiaalvõrgustikes suhtlemise ja internetiturvalisusega seotud probleeme. Kursuse läbis 80 õpetajat.

Kuna Eesti lapsed on Euroopa teiste riikide lastega võrreldes ühed noorimad, kes interneti kasutama hakkavad, siis on tähtis teha koostööd ka lasteaedadega. Tiigrihüppe Sihtasutus koostöös Audentese erakooliga korraldasid lasteaedade viimastele rühmadele õppekäigud, mille raames anti lastele esmasid teadmisi internetist ja arvutisuhtlusest, täideti töölehti ja vaadati õpetlikke multfilme.

Iga aasta veebruari teisel teisipäeval tähistatakse rahvusvahelist turvalise interneti päeva. 2011. aastal kandis päev juhtmötet „See on rohkem kui mäng, see on sinu elu“. Eestis korraldas Tiigrihüppe Sihtasutus turvalise interneti päeval õpetajatele konverentsi, kus käsitleti Eesti laste internetikäitumist, räägiti lapsevanemate ja õpetajate võimalustest muuta laste riskikäitumist ning tutvustada interneti positiivset sisu. Konverentsil rääkisid noored internetikasutajad oma kogemustest interneti kasutamisest ja sellest, mis tuge nad täiskasvanutelt ootavad. Lisaks korraldati noortele populaarsetel veebilehtedel kahenädalane kampaania, mille raames nad said testida oma teadmisi internetiturvalisusest. Veebiviktoriinis osales enam kui 7500 noort.

2012. aastal oli turvalise interneti päeva teemaks „Avastame digimaailma üheskoos – turvaliselt“, mis ärgitab mõtlema, kuidas saavad täiskasvanud ja lapsed üksteist virtuaalses maailmas toetada, et ohtu ei satuks kellegi privaatsus, maine ega tervis ja internetimaailmas toimetamine oleks positiivne kogemus. Kui aasta varem korraldati peamiselt õpetajatele ja sotsiaaltöötajatele mõeldud konverents, siis sel korral otsustati pöörata tähelepanu peredele. Perepäev „Targalt internetis“ toimus Tallinnas Lasnamäe linnaosa kultuurikeskuses Lindakivi, mis on populaarne koht eriti vene keelt kõneleva elanikkonna hulgas. Külastajad said osaleda mitmetes töötubades ja kuulata loenguid nii eesti kui ka vene keeles, lapsed leidsid tegevust teavituskeskuse loodud õppemänge katsetades ning Xbox 360 mängudes võisteldes. Noortele toimusid koostööpartnerite SA Vaata Maailma, Limparu ning EMT interaktiivsed töötöad. Avatud oli nõuandekohvik, toimusid viktoriinid ja õnneloos. Kinosaalet said kõige pisemad osalejad kaasa elada Jänku-Jussi seiklustele internetimaailmas või uudistada netilammaste toimetusi. Avatud olid „Targalt internetis“, vihjeliini ja abiliini infopunktid. Oma kogemusi ja häid nõuandeid jagas veebipolitseinik Andero Sepp.

Turvalise interneti päevast teavitamiseks anti 2011. aastal Õpetajate Lehe ja MTÜ Lastekaitse Liidu koostöös välja ajakirja „Märka Last“ eriväljaanne „Targalt Internetis“ ning 2012. aastal ilmus eriväljaanne ka Postimehe lisalehena. Eriväljaanded on leitavad projekti veebilehel.

Tiigrihüppe Sihtasutus korraldas koostöös Eesti Rahvusringhäälinguga 2. oktoobril 2011 telekanalil ETV2 teemaõhtu „Uus reaalsus“, kus näidati kolme dokumentaalfilmi: „Täiskasvanuks internetis“ (USA 2008), „Digirahvas“ (USA 2011) ja „Teine elu“ (USA 2011). Stuudioekspertide hulka, kes filme kommenteerisid, kuulusid nii projekti nõuandva kogu liikmed ja koolitajad kui ka noortepaneeli liige. Oktoobris korraldati Solarise keskuses projekti „Targalt internetis“ noortepäev, mis pakkus nii meelelahutust kui ka teavet internetiturvalisusest. Noortepäeval osales ligikaudu 400 noort ja täiskasvanut, kes täitsid teste ja ristsõnu, kuulasid loenguid ning mängisid Kinecti mängu.

Veebilehelt www.targaltinternetis.ee on leitavad kõik projekti jooksul koostatud õppe- ja teabe-

Kuna internet ei tunne riigipiire, siis on mujal üles laaditud materjal kättesaadav ka Eestis. Seega on illegaalse materjali leviku tõkestamiseks oluline rahvusvaheline koostöö riikide vihjeliinide vahel.

materjalid: koolitusmaterjal õpetajatele, eri vanuseastmele mõeldud tunnikavad (nt paroolid, privaatsus, varikontod, liigne arvutikasutus, kiusamine jne), plakatid „Netinipid“ ja „Seisa enda eest“, testid, ristsõnad, multifilmid, teabematerjalid lapsevanematele jne. Eriti populaarseks on osutunud netilammaste multifilmid, kus käsitletakse ohte ja riske, millega lapsed võivad kokku puutuda, ning antakse nõuandeid, kuidas neid vältida. Alles interneti kasutamist alustavatele lastele on loodud kolm Jänku-Jussi multifilmi, kus seletatakse, mis on internet, kuidas seal turvaliselt käituda ning kuidas luua head parooli.

Veebilehel on ka uus veebipõhine mäng Nastix (www.targaltinternetis.ee/nastix), mis on mõeldud peamiselt 9–14aastastele lastele turvalise internetikasutuse õppimiseks. Nastixiga koos saavad mängijad selgeks, mida ja kuidas oleks mõistlik internetis teistele esitleda, mis on privaatsus ja kuidas seda mõista interneti kontekstis, samuti õpitakse koos looma ja ära tundma turvalist parooli ning uuritakse, millele peaks tähelepanu pöörama uue kasutajakonto tegemisel. Viiruste küüsi langenud Nastixi arvuti ravitakse koos terveks ning hättasattunud mobiilikasutaja saab samuti abi. Eraldi mini-»»

» mängud on loodud küberkiusamise ning sotsiaalvõrgustikes suhtlemise teemadel.

Vihjeliin www.vihjeliin.ee

Jaanuaris 2011. aastal avas MTÜ Lastekaitse Liit koostöös Politsei- ja Piirivalveametiga veebilehe www.vihjeliin.ee, mille eesmärk on tõkestada laste õigusi, au, väärikut ja kehalist puutumatust rikkuvate materjalide levikut internetis. Veebilehe kaudu on internetikasutajal, kes märkab ebaseaduslikku materjali (laste seksuaalne ära-

Interneti kasutamise seotud pöördumiste puhul on küsitud eelkõige nõu, mida teha, kui laps on internetis kokku puutunud kahjuliku sisuga veebilehtedega (vägivald, pornograafia, suitsiid), mida teha küberkiusamise puhul või siis, kui tundmatu soovib lapsega suhelda *online*'is.

kasutamine, laste kaubitsemine (inimkaubandus jm)), võimalik sellest teada anda. Oodatud on teated ka muust alaealistele ebasobivast materjalist. Teabe saab edastada veebilehe www.vihjeliin.ee lihtsa vormi kaudu anonüümselt.

Vihjeliin avab saabunud teate, hindab selle sisu vastavalt Eestis kehtivatele seadustele ja kui see osutub ebaseaduslikuks, saadetakse teave edasi Politsei- ja Piirivalveametile. Eesti seaduste kohaselt on keelatud sellise teose (pildi, video jne) valmistamine, omamine ja levitamine, mis kujutab nooremalt kui kaheksateistaastast pornograafilises või nooremalt kui neljateistaastast last pornograafilises või erootilises situatsioonis.

Alates vihjeliini loomisest kuni maini 2012 on vihjeliinile edastatud 1353 teadet, millest 190 sisaldas viidet laste seksuaalse ärakasutamise materjalile. Peamiselt on ebaseaduslikku sisu esitavad veebilehed olnud välismaise pärituoluga, kuid mõni juhtum on puudutanud ka Eestis üles laaditud veebilehti. Kuna internet ei tunne riigipiire, siis on mujal üles laaditud materjal kättesaadav ka Eestis. Seega on materjali leviku tõkestamiseks oluline rahvusvaheline koostöö riikide vihjeliinide vahel. Alates 2011. aasta novembrist on Eesti vihjeliini INHOPE võrgustiku liige, mis ühendab 40 riigi vihjeliine.

Lasteabitelefoni 11 6111

Üleriigiline tasuta ööpäevaringne lasteabitelefoni 11 6111 alustas tööd 1. jaanuaril 2009. Eesmärk on anda igaühele võimalus teatada abi vajavast lapsest, tagada info edastamine vastavatele spetsialistidele ning pakkuda lastele ja lastega seotud isikutele esmast sotsiaalset nõustamist ning vajadusel kriisinõustamist. Teenuse osutamise seaduslik alus on lastekaitse seaduse § 59 esimene punkt, mille kohaselt on iga kodaniku kohustus viivitamatult teatada abi andvatele organitele abi vajavast ja hädas olevast lapsest.

Alates 2011. aasta märtsist pakutakse nõustamist ja abi ka interneti turvalisuse küsimustes, näiteks: kuidas arvutisõltuvust ära tunda, kuidas piirata lapse arvutikasutamist, identiteedivargus interneti sotsiaalvõrgustike kontodelt, soovitusel küberkiusamise puhuks jne. Nõu saamiseks on järgmised võimalused: helistada tasuta numbril 11 6111, *online*-kõned Skype'is (Skype'i kasutaja:

lasteabi_116111; kasutajaid ei lisata kontaktide hulka, helistamiseks ei pea olema kontaktiks lisatud), *online*-vestlus veebilehel www.lasteabi.ee, *online*-vestlus MSN Messengeris (kasutajanimi info@lasteabi.ee), personaalne kiri www.lasteabi.ee keskkonna kaudu, kirjutada otse info@lasteabi.ee.

Interneti kasutamise seotud pöördumiste puhul on küsitud eelkõige nõu, mida teha, kui laps on internetis kokku puutunud kahjuliku sisuga veebilehtedega (vägivald, pornograafia, suitsiid), mida teha küberkiusamise puhul või siis, kui tundmatu soovib lapsega suhelda *online*'is. Samuti on aktuaalsed privaatsusega seotud probleemid (identiteedivargus, isikuandmete avaldamine, isikuandmete väärkasutamine).

Siseriiklik ja rahvusvaheline koostöö

Projekti juures tegutseb noortepaneel, mille liikmed nõustavad meeskonda eelkõige noortele mõeldud tegevuste kavandamisel ja korraldamisel. Noortepaneeli liikmeteks on 15 noort vanuses 14–18 eluaastat, kes esindavad Tallinna Pelgulinna Gümnaasiumi, Tallinna Lilleküla Gümnaasiumi, Tallinna Ühisgümnaasiumi, Ehte Humanitaargümnaasiumi, Kohtla-Järve Gümnaasiumi, Valga Gümnaasiumi, Pärnu Sütevaka

Humanitaargümnaasiumi, Kuressaare Gümnaasiumi ja Põlva Ühisgümnaasiumi. Noortepaneeli liikmete kaudu jõuavad ürituste korraldajate ja materjalide koostajateni laste ja noorte arvamusel ja mõtted sellest, millist teavet nad interneti edukaks ja turvalisemaks kasutamiseks vajavad ning mil viisil see nendeni kõige paremini jõuab. Projekti raames toimunud koolitustel on noortepaneeli liikmed saanud teadmisi ja oskusi selle kohta, kuidas interneti turvalisemat kasutamist noorematele edasi anda – neid on nad ka edukalt rakendanud, korraldades oma koolis noorematele klassidele interneti turvalisemat kasutamist käsitlevaid üritusi. Noortepaneeli liikmed on Eestit edukalt esindanud ka mitmetel rahvusvahelistel üritustel.

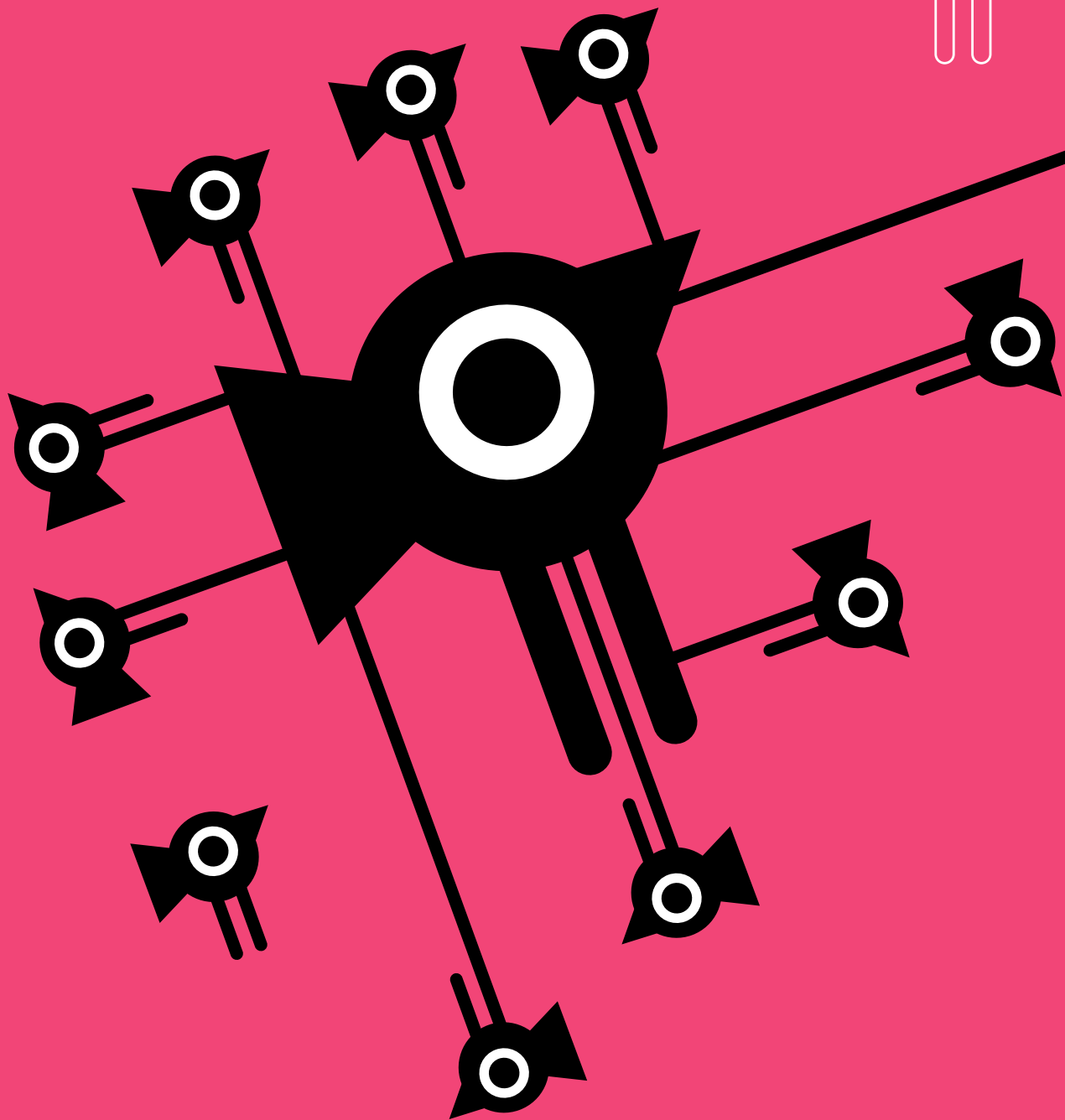
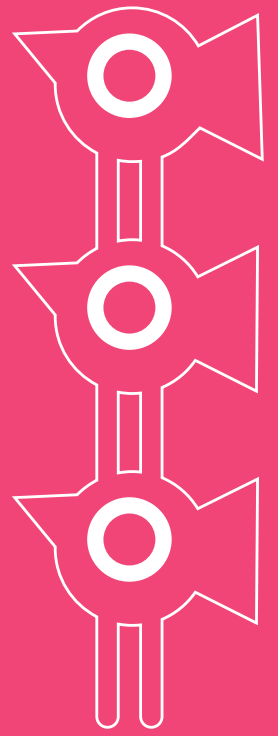
Projekti tegevuste elluviimiseks annab panuse ka nõuandev kogu, kus on esindatud Haridus- ja Teadusministeerium, Justiitsministeerium, Tartu Ülikool, Microsoft Eesti, Riigi Infosüsteemi Amet, EMT, Rate.ee, Eesti Lastevanemate Liit, informaatikaõpetajate Tallinna ühendus, Eesti Koolipsühholoogide Ühing, Eesti Infotehnoloogia ja Telekommunikatsiooni Liit, projekti Noortepaneel ja projekti partnerorganisatsioonide esindajad.

Lisaks siseriiklikule koostööle osaletakse ka rahvusvahelistes võrgustikes INSAFE, mis ühendab Euroopa turvalise interneti teavituskeskusi (www.saferinternet.org), ja INHOPE, mis on rahvusvaheline internetipõhiste vihjeliinide assotsiatsioon (www.inhope.org).

Projekti elluviimist toetab 75% ulatuses Euroopa Komisjoni programm „Safer Internet“ („Turvalisem internet“), millega on ühinenud 27 Euroopa Liidu liikmesriiki ning Norra, Island ja Venemaa.

Projekti „Targalt internetis“ jätkuprojekt alustab 2012. aasta juunis ja kestab 2014. aasta oktoobrini. Selle raames on plaanis jätkata laialt ulatusliku koolitustööga, luua uusi huvitavaid teavitusematerjale, anda välja interneti turvalisema kasutamise e-õpik, korraldada õpilastele mitmeid temaatilisi võistlusmänge ja interaktiivseid üritusi-konverentse, korraldada kampaaniaid jpm. Enam plaanitakse teha koostööd ka sotsiaaltöötajatega, noortekeskuste, Tartu laste tugikeskuse, Andmekaitse Inspeksiooni jt laste turvalisemat internetikasutust edendavate organisatsioonidega. Jätkub vihjeliini ja abiliini töö. Rohkem infot leiate projekti veebilehelt www.targaltinternetis.ee.







4. PEATÜKK

KIIRE INTERNET

Internetist on saanud tänapäeva ühiskonna toimimise üks olulisemaid eeldusi: ligipääs sellele on elutähtis nii majanduskasvu tagamiseks kui ka inimeste heaolu suurendava ühiskonna arendamiseks. Uuringufirma McKinsey andmetel aitab lairibaühenduste kasutuselevõtu 10% kasv majapidamistes suurendada sisemajanduse kogutoodangut 0,1–1,3%. Nõnda on kiire interneti arendamine esmatähtis ülesanne nii Euroopas kui ka mujal maailmas. Näiteks seab Euroopa infoühiskonna arenguid suunav dokument, digitaalarengu tegevuskava, eesmärgiks, et 2020. aastaks oleks kõigil eurooplastel vähemalt 30 Mbit/s kiirusega internetiühendus ning pooltel kodumajapidamistel ligipääs vähemalt 100 Mbit/s kiirusega ühendustele. See peatükk räägib sellest, mida Eestis interneti kättesaadavuse parandamiseks ja kiirete internetiühenduste tagamiseks tehakse.



Eesti kogemus lairibaühenduste arendamisel



OLAV HARJO

olav.harjo@elasa.ee

Eesti Lairiba Arendamise Sihtasutus

Euroopa 2020 tegevuskava lipuprojekt „Euroopa digitaalne agenda“ seab eesmärgiks katta kogu Euroopa selleks ajaks kiire internetiga. Kõikidele kodudele, ettevõtetele ja asutustele Euroopa Liidus peab olema tagatud võimalus liituda vähemalt 30Mbit/s internetiühendustega ning vähemalt pooltel peab olema juurdepääs 100Mbit/s ja kiirematele internetiühendustele.

Ka Eesti on võtnud endale eesmärgiks tagada kõigile võimalus liituda uue põlvkonna lairibavõrguga. Selle eesmärgi ning tegevuskava töötasid Majandus- ja Kommunikatsiooniministeerium (MKM) ja Infotehnoloogia ja Telekommunikatsiooni Liit (ITL) välja juba 2009. aastal ning see pandi kirja „Eesti uue põlvkonna lairibavõrgu arendusvisiooni“ dokumendis.

Alates 2009. aastast on lairibaühenduste rajamine Eestis hästi edenenu. Suuremates linnades on tänaseks kiired internetiühendused juba laialt saadaval. Sideettevõtjad on ehitanud välja uusi fiiberoptilisi võrke ning võtnud kasutusele uusi tehnoloogiaid ja seadmeid. 100Mbit/s ja kiiremad ühendusi saavad kasutada juba pooled majapidamistest-ettevõtetest-asutustest, seda nii FTTH kui ka DOCIS 3 tehnoloogiate kaudu. Jõudsalt areneb ka mobiilne internet, kus andmesidemahud eelmisel, 2011. aastal, neljakordistusid – veelgi suuremat arenguhüpet on oodata 4G-tehnoloogiate levikuga.

Seega kohtades, kus on küllaldaselt potentsiaalseid kliente, turg toimib ning sideettevõtjad tagavad ka kiired lairibaühendused kõikidele soovijatele.

Lairibaühendused maapiirkondadesse

Eesti keskmine elanike tihedus on ca 30 inimest ruutkilomeetri kohta. Maapiirkondades on elanikke aga isegi alla 10 inimese ruutkilomeetri kohta. Seega ei saa eeldada, et turutingimustel jõuaks kiire internet Eesti maapiirkondadesse. Samas on riik huvitatud, et elu oleks ka mujal kui meie suuremates linnades – et kõikjal Eestis oleks võimalik elada, töötada ja haridust saada. Selleks et inimesed sooviksid elada ka väljaspool suuri keskusi, peab neile olema loodud kvaliteetne elukeskkond, töökohad, hariduse saamise võimalus. Täna ei saa ükski ettevõtte ega asutus toimida ilma internetiühenduseta. Samuti ei kujuta enam keegi ette haridus- või teadusasutust ilma kiire internetiühenduseta. Olgu see põhikool või ülikool, ilma selleta pole lihtsalt enam võimalik haridust anda või teadust teha.

Ka inimeste elukeskkond ei ole enam nii kvaliteetne, kui puudub kiire internetiühendus: puudub juurdepääs paljudele teenustele, samuti ei ole võimalik kasutada tänapäevaseid suhtlusvahendeid ning ka infoühiskonnas osalemine on

piiratud. Kiired lairibaühendused on üks maapiirkondade arengu alustala.

Projekti EstWin areng

Selleks et kiired lairibaühendused jõuaksid ka Eesti maapiirkondadesse, alustasid MKM ja ITL 2009. aasta kevadel projektiga EstWin.

Projekti mudel on unikaalne: ühiselt tegutsevad nii riik kui ka muidu omavahel konkureerivad sideettevõtjad. Riik toetab ELi toetusfondide vahenditest fiiberoptilistel kaablitel põhineva baasvõrgu väljaehitamist kõikidesse asulatesse. Sideettevõtjad tagavad teenuste pakkumise lõpptarbijatele ning ka baasvõrgu jätkusuutliku majandamise.

EstWini projekti elluviimiseks asutasid 8 ITLi liiget Eesti Lairiba Arendamise Sihtasutuse (ELA). ELAs saavad kokku kõikide osapoolte, ministeeriumite, kohalike omavalitsuste, kogukondade ja sideettevõtjate huvid ja nad kõik on kaasatud ka baasvõrgu planeerimisse.

ELA ülesanne on planeerida baasvõrk, lähtudes kõikide osapoolte soovidest, samuti korraldada baasvõrgu ehitamise finantseerimine ning see võrk välja ehitada. ELA on ka väljaehitatud baasvõrgu omanik ja operaator. Nii et ELA ülesanne on tagada ka võrgu kättesaadavus ning selle jätkusuutlik majandamine.

EstWini alguses kaardistati kõik maapiirkondades olevad fiiberoptilised võrgud ning selgitati välja sideettevõtjate plaanid uute võrkude rajamiseks. Selle tulemusena leiti turutõrke piirkonnad ning valmis esialgne plaan, kuhu tuleb EstWini projektiga võrk rajada. Kokku tuleb ehitada üle 6000 kilomeetri võrku.

Detailne võrgu planeerimise protsess on aga palju keerulisem ja aega nõudvam. Sellesse on kaasatud palju osapooli ning kasutatakse eri infot. Elanike ja majade paiknemise väljaselgitamiseks kasutatakse aadressregistrit. Kokku on kogutud kõikide koolide, raamatukogude, rahvamajade, noortekeskuste jms paiknemise info, samuti on saadud kõikidest kohalikest omavalitsustest soovid ühenduskohtade kohta. Kogu info olemasolevate võrkude, sidesõlmede, mobiilimastide ja riigile oluliste objektide kohta on ka toodud spetsiaalselt lairibavõrgu planeerimiseks loodud kaardirakendusse. Lisaks kasutatakse infot nii Maanteeameti planeeritud teetöö-

de kohta (kuna suurem osa kaableid paigaldatakse teedele) kui ka teiste infrastruktuuri arenguplaane. Kõige selle alusel valmivad umbes 30–50 kilomeetri pikkused töödeprojektid, mis kooskõlastatakse kõikide osapooltega. Lõplikud otsused iga projekti kohta teeb ELi toetusfondi rakendusasutus, kelleks on EstWini projektide puhul olnud RIA, PRIA ja EAS. Rahastamisaotlusi on esitatud 58 projekti elluviimiseks.

Valminud võrgud

EstWini võrk on jõudnud juba 77 kohaliku omavalitsuse territooriumile. Valminud on ligi viiendik planeeritud võrgust ehk umbes 1200 km. Välja on ehitatud 420 võrguga liitumispunkti. Projekteerimise ja ehitamise järgus on aga veel ligi 1300 km ulatuses võrku, mis valmis 2012. aasta sügisel. Kogu valmis võrk on detailselt kirjeldatud võrguregistris, samuti on loodud vajalikud vahendid võrguinfo saamiseks nii võrguhaldajale, sideettevõtjatele ja teistele seotud isiku-

Inimeste elukeskkond ei ole enam nii kvaliteetne, kui puudub kiire internetiühendus. Kiired lairibaühendused on üks maapiirkondade arengu alustala.

tele. Kogu valmis ja ehitusel olev võrk on nähtav kõigile lehel <http://ela12.elasa.ee/elakaart>.

Järgmiseks etapiks on juba ette valmistatud planeering 1500 km võrgule, mida loodetakse hakata välja ehitama 2013. aastal. Kui võrgu edasine areng toimub plaanide järgi, siis valmib kogu EstWini võrk hiljemalt 2015. aasta lõpuks.

Valmis võrgul on 24/7 monitooring, tagatud on kiire rikete likvideerimine. Vastavalt võrgu hooldajaga sõlmitud kokkuleppele peavad kõik võrgu rikked olema likvideeritud hiljemalt kuue tunni jooksul. Kuna tegemist on tehnoloogiliselt kaasaegse võrguga ning kogu võrk on detailselt dokumenteeritud, siis on tegelikkuses rikete tõenäosus väike. 2011. aasta jooksul toimus võrgus ainult üks rike, mis põhjustas ajutise sidekatkestuse ja ka see oli põhjustatud inimlikust eksimusest.

Võrku saavad kasutada kõik sideettevõtted ja riigiasutused võrdsetel tingimustel. See tähendab, et võrk on kõikide soovijate jaoks ühiskasutusel. Kuna ELA on kasumit mittetaotlev organisatsioon, »»

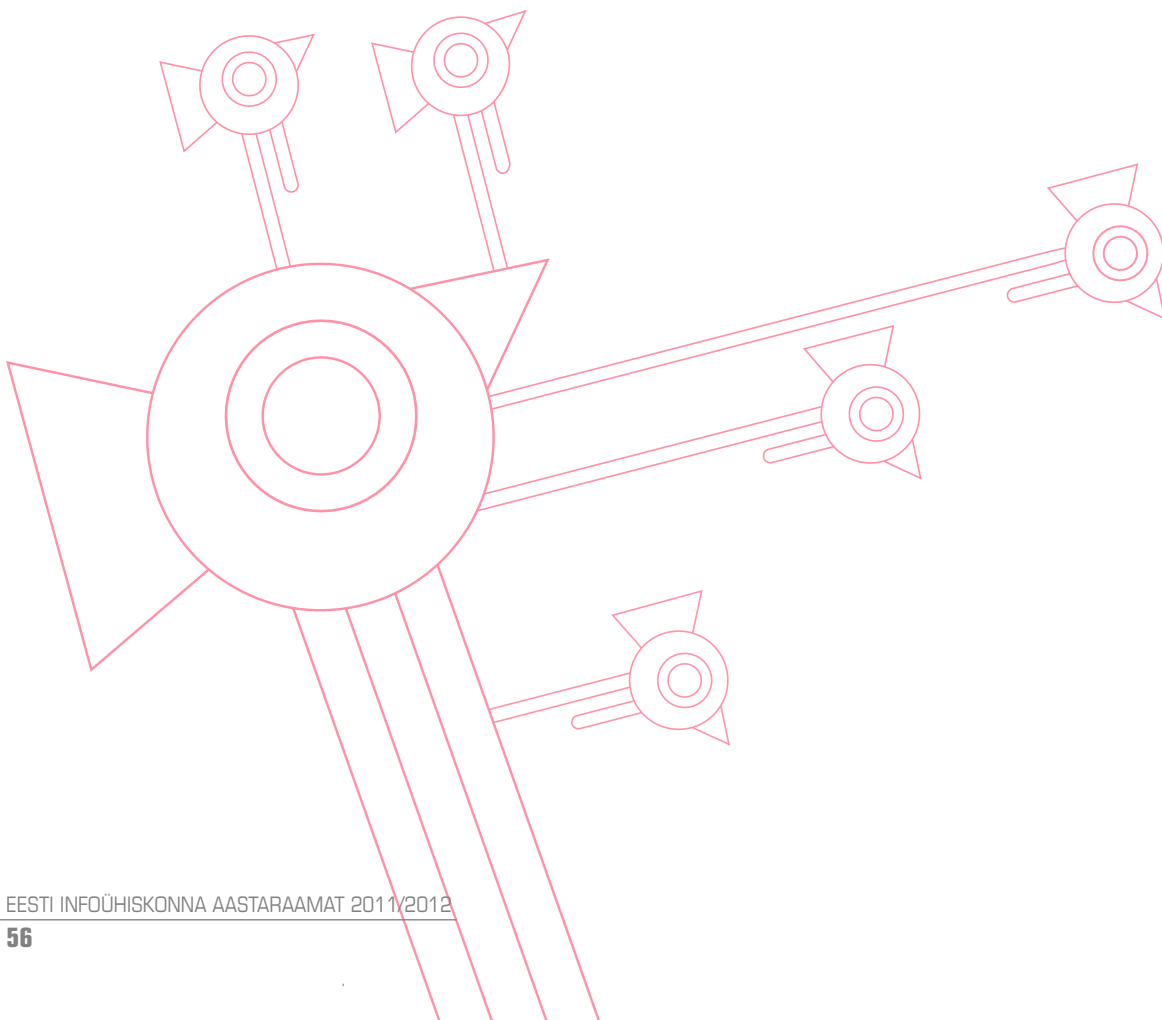
» siis peavad võrgu kasutajad ühiselt tasuma ainult võrgu ülalpidamise kulud ning omafinantseerimisega seotud finantskulud. Tänu sellele on võrgu kasutamise tasud väiksed ning sideettevõtjatel on võimalik pakkuda kiiret interneti ka piirkondades, kus potentsiaalseid kliente on väga hõredalt. Praeguseks on sõlmitud juba ligi 200 tootelepingut võrguosade kasutamiseks.

Rahvusvaheline huvi

EstWini projekt on tõestanud, et üleriigilist lairibavõrku on võimalik kiiresti arendada, kui on olemas selge eesmärk, arvestatakse kõikide osapoolte huvidega ning on olemas tugev or-

ganisatsioon, kes projekti ellu viib. Meie edu ei ole jäänud nähtamatuks ka teistes ELi riikides. Meie tegevusmudeli vastu on nimelt huvi tundnud mitmed riigid, kes samuti soovivad kiireid lairibaühendusi arendada, näiteks Läti ja Soome, aga ka kaugemad riigid, nagu Poola, Hispaania ja Itaalia.

Kuigi kõikide riikide probleemid ja võimalused on erinevad, on meil kindlasti midagi, mida teistele edasi anda. Meie EstWini projektist saadud kogemused võiksid olla üheks eksporditavaks ELi maadesse, kes soovivad kiireid lairibaühendusi arendada.



4G – Eesti mobiilse interneti võimalused ja edulugu



ANDO MEENTALO

ando.meentalo@emt.ee

AS EMT

Kui Eesti riik väljastas 17. detsembril 2010 esimese 4G konkursi tulemusel sagedusload, püstitati Eestis mitteametlik maailmarekord – EMT 4G-võrk käivitati ja anti kasutajate kätte kuus minutit pärast loa väljastamist! Esimeseks kliendiks sai Eestile kohaselt IT-visionäär Linnar Viik.

EMT võrk oli maailmas järjekorras üheteistkümnendane 4G-võrk. Oluline oli see, et riik valis litsentsi väljastamisel mõelduka litsentsitasu ning operaatoreid pidid vastutasuks garanteerima võrgu kiire väljaehitamise. Tulemus: eeldatavasti on juba aastal 2014 kogu Eesti kaetud uue põlvkonna mobiilse lairibavõrguga. Kiirustega, millest paljudes piirkondades sai seni vaid unistada.

Kiirest ühendusest sai edu võtmetegur

Mobiilse interneti aeg algas Eestis oktoobris 2005 EMT 3G-võrguga. Kui 2003 tehti esimesed 3G-testid, siis peamine nähtav erinevus tundus olevat videokõne. Teenuse reaalsel käivitamisel aastal 2005 olid kõige populaarsemad rakendused aga juba liikluskaamerate vaatamine ummikutest möödalaveerimiseks ning mobiilTV telefoni väiksel ekraanil. Täna aga on tegelik 3G-mobiilside edufaktor mobiilne internet: kiire lairibaühendus kõikjal üle Eesti ja välisriikides sama seadmega ja laialdaste teenustega.

Netikasutus suurel arvutikraanil oli käivitamise ajal veel kasutajate soovidest maas. Kiirem kasv

algas aastal 2007, kui leviala kaardil oli saanud nii suureks, et torkas silma ning arvutiga ühendatavate seadmete hind muutus taskukohaseks. Vähem oluline ei olnud ka see, et mobiilse interneti kasutusmugavus ei eeldanud enam IT-haridust, sest varasemate seadmete kasutamine oli justkui võitlus arvuti riistvara ja tarkvaraga. Nüüd aga sai USB-modemiga hakkama igaüks.

Edasine oli juba kiiruste kasvamise aeg. Veebisurfamiseks olid kiirused piisavad, kuid multimeedia aeg YouTube'i ja uudisteportaalides laetavate videouudistega andis aimu, et peagi jäävad 3G-võrgud nõudlikele kasutajatele kitsaks.

2009. aasta lõpus käivitas TeliaSonera esimesed kaubanduslikud 4G-võrgud Põhjamaades ning juba 2010. aasta veebruaris avas nende gruppi kuuluv EMT esimese LTE-tehnoloogial baaseeruva testvõrgu. Uus võrk pakkus igale soovijale kiirust kuni 100 Mbit/s. Siit jäid käivituseni juba vaid loetud kuud.

Kindlasti ootame suurt abi selle võrgu laiendamisel riigiga ühiselt arendatavast EstWini projektist. See peaks võimaldama meile just asulatevõrgude jaamade tarbeks kiired baasühendused. On ju teada, et 4G-tehnoloogia areneb lähiaastail lisaks levile ka kiirustes, kiirusteni 1 Gbit. Selliseid kiiruseid suudab tugijaamadeni kanda vaid fiiberoptiline baasvõrk. Ei ole võimatu, et juba 2014. aasta lõpuks on enamik Eesti territooriumist kaetud 4G-võrgu levialaga. »

» Mida tõi Eestile 4G-võrk?

Kindlasti tekitas huvi asjaolu, miks sai ühe esimese 4G-jaama endale Kohila, asula, mis paikneb väljaspool metropole ja pole isegi maakonnakeskus. „Kas seal elab kellegi hea tuttav?“ oli sage küsimus. Tõde on aga see, et seal elavad uusrajoonides inimesed, kes vajavad kiiret interneti ning kes seda seni ei saanud. Nende jaoks see võrk ju ehitataksegi!

Reaalselt on 4G ainuke tehnoloogia, millest võib eeldada, et see toob Eesti kodudesse, eriti just hõreasustusega aladel, kümnete megabittide kiirusega internetiühenduse. Sest on ebareaalne, et samalaadse kiirusega fiiberoptika või vaskpaariga teenused jõuavad igasse kodusse.

Nagu enne mainitud, hakkas 3G-võrgus enim häirima see, et pole võimalik kasutada tuleviku kõrgresolutsiooniga mobiilseid multimeediateenuseid. 4G võimaldab tuua kasutajale ka suurele ekraanile digiTV teenused samas kvaliteedis nagu kaabelside pakkujad. Tänapäevane 3G võimaldab tehniliselt selliseid teenuseid pakkuda kvaliteetselt väikestel nutitelefonide ekraanidel, kuid 4G toob meie kõigini Triple Play: telefon, internet ja TV koos. Eeldatavasti jõuavad esimesed hea valikuga mobiilse TV teenused turule juba 2013. aastal.

Video, TV, online-mängud

Videosisu tarbimisele annab kindlasti hoogu ka seadmete areng, mis on toonud kasutajateni ka 4G toega tahvelarvuti. Need on mugavad internetis surfamiseks, kuid toimivad edukalt ka täiendava ekraanina nii kodus kui ka lastele autos filmide näitamisel.

Samalaadset huvi 4G vastu tunnevad ka video ja pildisisu pakkujad, et tuua uudised kiirelt vaatajateni ilma satelliitülekandejaama ja kaablit tellimata. Ka metsatalu valvekaamera võib leida ainukesel sobiva ühenduse just 4G-võrgu abil.

Äriettevõtetele pakub 4G huvi seoses kiirete internetiühendustega ka oma tootmisettevõtetes-

se, enne kui sinna jõuab kaabliga püsiühendus. Praktikaks võibki jääda toimima vaid traadita 4G-ühenduse põhjal, mis vaid mõni aasta tagasi näis ebareaalne.

Peagi näeme ka nutitelereid, mis kasutavad ühenduseks TV ja interneti teenustega pesa SIM-kaardi jaoks. Ainuke juhe, mida 4G-televisoor vajab, on 220 V toitejuhe. Ulme? Ent see polnudki ju nii ammu, kui WiFi televisooris veider tundus. Siis sai WiFi osta lisaseadmena – nüüd on see uute telerite loomulik osa.

Üks seltskond, kes on mobiilsesse interneti suhtunud pragmaatilise umbusuga, on kasvav *online*-mängurite kogukond. Olukorras, kus mängukonsoolid ja arvutis mängitavad mängud eeldavad head reaktsiooni vastasmängijate edestamiseks, ei tundunud 3G piisavalt ergas. 4G lahendab ka selle mure, pakkudes sama häid võimalusi kui ükskõik millised konkureerivad tehnoloogiad.

Äsja tuli ka uudis, kus räägiti juhita sõitvast autost, mis ammutab infot internetist. Kindlasti eeldab selline auto kiiret infoedastust, mis parandab juhtimise kvaliteeti. Kujutage ette, kui palju infot oleks Eesti oludes autosse edastada asfaldiaukudest. Kindlasti ei saa unustada, et ka juht eeldab kvaliteetset interneti ja lisateenuseid – miks mitte edastada sõpradele sõites reaalajas kõiki neid ilusaid vaateid, mis autoaknast avanevad?

Mis saab edasi? 4G/LTE-tehnoloogia areneb lisaks levialale ka kiirustesse. Kindlasti ei ole sadadesse megabittidesse ulatuvad kiirused ka reaalsuses lähiaastail utopia. Laieneb ka seadmete valik.

4G ei piirdu ainult Eestiga. Maailm muutub kindlasti palju väiksemaks ning 4G/LTE on tehnoloogia, mis levib ühtmoodi nii Euroopas kui ka Ameerikas ning Aasias. On oluline, et Eesti teenusepakkujad ja tarkvaraarendajad ning loomulikult kliendid ei mängi ajalist edu maha ning on 4G võimaluste kasutamisel esirinnas.



4G mobiilne internet maapiirkondadesse



ANDRUS KAARELSON

andrus.kaarelson@elisa.ee
Elisa Eesti AS

Tänaseks on kõik operaatorid avanud 4G-tugijaamad 2600 MHz sagedusalas. Sel sagedusel on Elisa avanud 4G-testvõrgud viies Eesti linnas: Tallinna, Pärnu, Viljandi, Haapsalu ning Tartu kesklinnas.

Aga kuna see sagedusala on väga piiratud leviulatusega, on neil 4G-tugijaamadel tulevikus pigem toetav funktsioon mahtude läbilaskevõime suurendamisel. Kõik operaatorid ootavad pikisilmi 800 MHz sagedusala tegevuslitsentside konkurssi, mis peaks toimuma 2013. aastal. Uue tehnoloogia abil saavad operaatorid 4G-võrgu viia igasse Eestimaa nurka.

Elisa on juba alustanud 800 MHz sagedusala testimist. Märtsis avati esimesed testlevialad Võrumaal Kobela alevikus ja Haapsalus. Kõik Elisa edasised 4G arendamise plaanid ongi suures osas rajatud 4G 800 MHz sagedusalale. See sagedus võimaldab kiirelt ja efektiivselt välja ehitada kogu Eestit katva ülikiire mobiilse interneti teenust pakkuva 4G-võrgu.

Selles sagedusalas hakkab Elisa koostööd tegema ka niigi ellu kutsutud EstWini projektiga. EstWin ja mobiilne internet on omavahel tihedalt seotud. Viimased poolteist kilomeetrit internetiühendusest kliendi koduni saab välja ehitada väga hästi hoopis mobiilse interneti toel, mis on kliendile palju soodsam lahendus.

2009. aasta aprillis ITLi koostatud ja valitsuse heaks kiidetud „Eesti uue põlvkonna lairibavõrgu arendusvisioon“ püstitab eesmärgi, et 2015. aasta lõpuks peab kõikidele kodudele, ettevõtete-

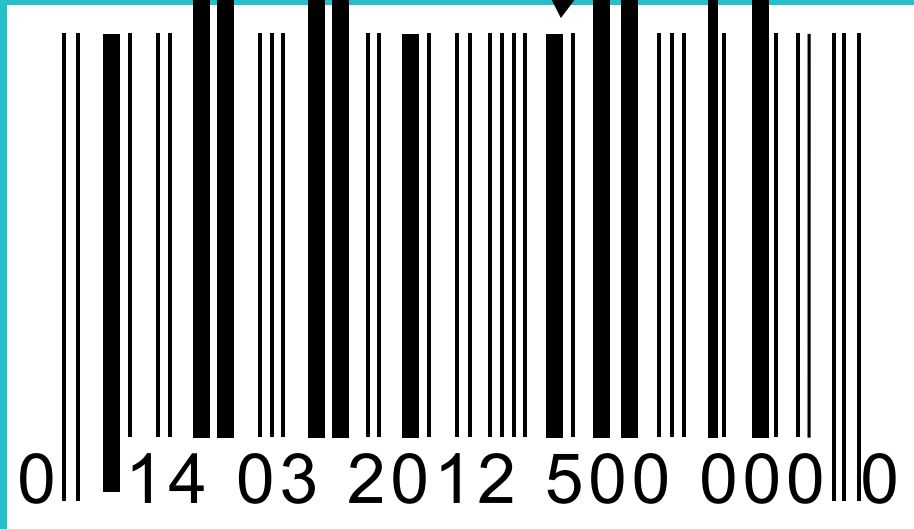
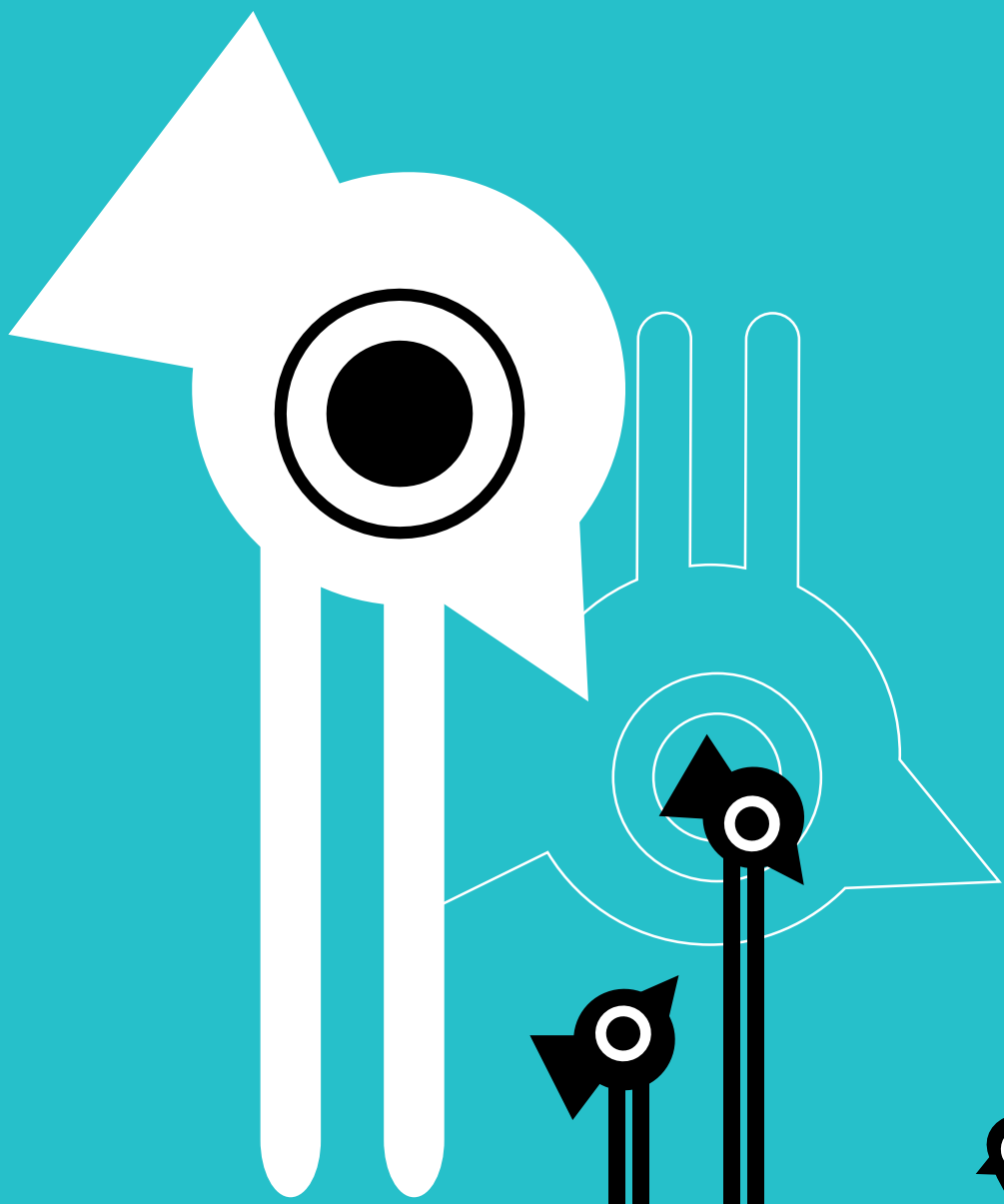
le ja asutustele olema kättesaadav 100 Mbit/s andmesidekiirust võimaldav lairibaühendus. Selle eesmärgi saavutamine on otseses sõltuvuses EstWini projektist. Aastaks 2015 saab valmis fiiberoptiliste kaablite võrk, mis jõuab kõikide asulate ni Eestis. Selle tulemusena peab 98% majapidamistest, ettevõtetest ja asutusest olema võrgule lähemal kui 1,5 km.

LTE 800 MHz on tehnoloogia, mis võimaldab maapiirkondades katta viimased 1,5 kilomeetrit klientide ja Eesti Lairiba Arendamise Sihtasutuse arendatud fiiberoptilise kaablivõrgu vahel ning viia ülikiire internetiühendus igale kliendile koju või kontorisse. Lisaks sellele, et EstWini toel jõuab eraklientide maakodudesse internet, vajavad kiiret internetiühendust äriettevõtted ja avaliku sektori organisatsioonid, näiteks koolid, raamatukogud, omavalitsused.

Võrreldes üle-eelmisel aastal jagatud LTE 2600 MHz sagedusega võimaldab 800 MHz palju kiiremini Eesti kiire internetiga katta, sest selleks on vaja ligi viis korda vähem tugijaamu kui 2600 MHz puhul. Madalam sagedus tagab ka märgatavalt parema siselevi hoonetes, tänu millele saab klient nautida kvaliteetsemat teenust ja märgatavalt suuremaid internetiühenduse kiiruseid.

Neljanda põlvkonna LTE (Long Term Evolution) standardil põhinev võrk võimaldab klientidele tulevikus pakkuda ülikiiret mobiilset interneti. Uudse tehnoloogiaga 4G-võrk tõstab mobiilse andmeside allalaadimiskiirused kuni 100 Mbit/s ning üleslaadimiskiirused kuni 50 Mbit/s.







5. PEATÜKK

E-IDENTITEET

2012. aasta jaanuaris möödus juba 10 aastat esimese ID-kaardi väljaandmisest Eestis. Praegu võib öelda, et 1990. aastate lõpus tehtud otsus – võtta kasutusele universaalsed sertifikaadid – on end õigustanud. ID-kaart ei ole enam juba aastaid üksnes täiendav isikutuvastusvahend, vaid turvaline tööriist, mida kasutavad usinalt oma teenustes ja IT-lahendustes nii avalik kui ka erasektor. Avaliku võtme infrastruktuur (Public Key Infrastructure – hõlmab digiallkirja andmiseks ja kontrollimiseks vajaminevaid teenuseid) ja ID-kaart on riigi infosüsteemi nurgakivid, millel põhineb suurel määral ka Eesti e-riigi rahvusvaheline maine. See peatükk annab ülevaate Eesti eID ökosüsteemist ning selle olulisematest komponentidest, nagu digitempel, mobiil-ID ja digi-ID. Peatüki viimases artiklis vaadeldakse digitaalalkirjaga seotud probleeme Euroopa ühtse turu kontekstis. Kindlasti on asjakohane enne peatükiga tutvumist heita pilk ka 10 aasta tagasi aastaraamatus avaldatud artiklile, mis räägib ID-kaardist (www.riso.ee/et/pub/2002it/).



Kümme aastat eID ökosüsteemi



TARVI MARTENS

tarvi.martens@sk.ee
AS Sertifitseerimiskeskus



MARK ERLICH

mark.erlich@ria.ee
Riigi Infosüsteemi Amet



TAAVI VALDLO

taavi.valdlo@riso.ee
Majandus- ja Kommunikatsiooniministeerium



UUNO VALLNER

uuno.vallner@riso.ee
Majandus- ja Kommunikatsiooniministeerium

Elektroonne identiteet (eID) on Eestis kujunenud kümne aastaga iseorganiseeruvaks ökosüsteemiks. Sajandivahetuseks olid siin välja kujunenud tugevad turvaekspertide koolkonnad ülikoolides, avalikus ja erasektoris. Ühed aktiivsemad huvipooled olid pangad ja telekommunikatsioonifir-

mad. Osapoolte ühiseks huviks oli reaalselt toimiva avaliku võtme infrastruktuuri (PKI) loomine ja selle kaudu elanikkonnale ning ärile uute võimaluste tekitamine. Tollased ideed said poliitilisteks otsusteks ning löid pinnase era- ja avaliku sektori koostööle. Praeguseks on kehtiv ID-kaart ligi 1,2

miljonil inimesel, kellest umbes 85% on Eesti kodanikud ning 15% välismaalased. Kümne aasta jooksul on kokku antud 72,6 miljonit digiallkirja ning vähemalt korra on dokumenti elektrooniliselt kasutanud pea pooled ID-kaardi omanikud.

Asutused on hakanud aru saama digiallkirjastamise eelistest. Nii näitab Sertifitseerimiskeskuse ja MoZg Agentuuri uuring¹, et digiallkirjastamine võimaldab Eltel Networksil igakuiselt kokku hoida 1380 eurot ja Tartu Ülikoolil 11500 eurot, mis teeb viimasel juhul nelja aasta peale üle poole miljoni euro. Seejuures on suurim kokkuhoid tööjõukuludelt, samuti printimise- ja postikuludelt.

Avaliku võtme infrastruktuuri ülesehitamisel tuleks turvalisuse huvides ökosüsteemi komponendid võimalikult tugevalt hajutada. Hajutamine tagab protsesside läbipaistvuse ja väldib monopoolsete, tsentraliseeritud süsteemidele omaid nõrga lüli (*single point of failure*) ohte.

Avaliku sektori jaoks on eID üks prioriteete. Elektrooniline asjaajamine on haldusmenetluses võrdstatatud kirjalikuga. Digitaalset isiku tuvastamist ja digitaalalkirja kasutatakse haldusmenetluses laialdaselt. Eesti soovib olla jätkuvalt üks selle ala juhtriike Euroopas, osaledes mitmetes rahvusvahelistes projektides, nagu STORK ja e-CODEX.

Projektiga STORK (Secure idenTity acrOss boRders linKed) luuakse kogu Euroopa Liitu hõlmav elektrooniliste identiteetide (eID) koosvõime platvorm. Meie ekspertide osalemine jätkuprojektis STORK 2.0 tagab Eesti ettevõtjatele turvalise juurdepääsu Euroopa internetipõhistele süsteemidele ja samas lubab ka Euroopa ettevõtjatel elektrooniliselt kasutada e-riigi ning erasektori infosüsteeme ja portaale. Euroopa Liidu piiriülese IT-projekti e-CODEX eesmärgiks on muuhulgas luua võimalused elektroonilise isikutunnistuse ja digiallkirja alaste lahenduste kasutamiseks digitaalsel piiriülesel kohtumenetlusel.

Kes on kes eID ökosüsteemis?

Isikud on ökosüsteemi kõige olulisemad osalised. See, kuidas elanikkond võtab vastu uued lahendused, mõjutab kogu ökosüsteemi arengut. Igal isikul on olemas identiteet ehk teadmine endast. Osa sellest teadmisest annab isik teistele osapooltele, kellega lepitakse kokku isikut identifitseerivas nimes/identifikaatoris, nt saidi konto, panga arvelduskonto, isikukood suhtlemisel riigiga. Eriti tähtis on isikul avada osa oma identiteedist sõltumatule kolmandale osapooltele, nt

riigile või sertifitseerimisasutusele. Isik annab riigile enda kohta sellised andmed (nime, pildid vms), mis lubavad isikut üheselt identifitseerida. Riik omistab isikule unikaalse identifikaatori (isikukoodi) ja väljastab n-õ paberi (passi, ID-kaardi vms). Sellist identiteeti seotuna nn kvalifitseeritud sertifikaadiga saab kolmas osapool kasutada digitaalseks isikusamasuse tõestamiseks.

Digitaalmaailmas tõestab inimene oma seotust identifikaatoriga paroolide, PIN-koodide, sertifikaatide jms abil. Eesti seadusandluse kohaselt tõestab isik digimaailmas oma seotuse identifikaatoriga kvalifitseeritud sertifikaadi abil. Eestis on isiku baassertifikaadiks ID-kaardile kantud sertifikaadid isiku digitaalseks tuvastamiseks ja digitaalseks allkirjastamiseks.

Lisasertifikaadi saamiseks valib inimene sertifitseerimisteenuse pakkuja, saab sertifikaadi ja aktiveerib baassertifikaadiga selle teenusepakkuja sertifikaadi.

Asutused. Teiseks oluliseks ökosüsteemi komponendiks on asutused. Asutuste tahe aktsepteerida digiallkirju ja luua süsteeme, mis toetavad sertifikaadipõhist autentimist ja allkirjastamist, on olnud Eesti üks edu võti. Üheks eestvedajaks on siin olnud avalik sektor, digitaalalkirja seadus² **kohustab asutusi aktsepteerima digitaalalkirjastatud dokumente.**

Politsei- ja Piirivalveamet (PPA) on eID ökosüsteemi olulisemaid toimijaid. PPA vastutab residentide identiteedi omistamise ja haldamise eest. Avaliku võtme infrastruktuuri osas on PPA rollid järgmised:

- annab välja isikutunnistusi (ID-kaart) ja digitaalseid isikutunnistusi ning tagab nendele sertifitseerimisteenuse osutajate väljaantavate kvalifitseeritud sertifikaatide lisamise;
- tagavad aktiveerimisteenuse kaudu kodanikele võimaluse oma eID seostada/aktiveerida kvalifitseeritud sertifitseerimisteenuse pakkuja sertifikaatidega.

Eesti oludes katab PPA elanike baassertifikaadi elutsükli kulud, tagades isikutele sellega nende tasuta haldamise, samuti vastutab ta turvalise allkirja andmise vahendi (kaardi, kiibi, kiibi operatsioonisüsteemi, krüptoalgoritmide jms) turvalisuse ja nõuetele vastavuse eest.

Sertifitseerimiskeskus (SK). Digitaalsete usaldusteenuste osutajad annavad välja kvalifitseeritud sertifikaate ja pakuvad digitaalseid usaldus-»

» teenuseid. Digitaalmaailmas on usaldusteenuste osutajad PKI infrastruktuuri südameks. Kvalifitseeritud sertifikaatide puhul peab sertifitseermisteenuse osutaja tagama kodanikule võimaluse aktiveerimise kaudu seostada väljaantud sertifikaat PPA hallatava eIDga. Eestis on põhiliseks teenusepakkujaks AS Sertifitseerimiskeskus (SK).

2001. aastal asutatud Sertifitseerimiskeskus on riiklikult akrediteeritud ettevõtte, mis on kesken-
dunud sertifitseerimis- ja ajatempliteenusele ning sellega seotud tarkvara arendusele ja opereerimisele. SK asutajad ja omanikud on võrdsetes osades Swedbank, SEB Pank, AS EMT ja AS Elion Ettevõtted. SK põhitegevused:

- sertifitseerimis- ja ajatempliteenuse pakkumine,
- digitaalallkirjastamise tehnoloogia ja rakenduste väljatöötamine,
- valideerimisteenuste pakkumine,
- konsultatsiooniteenused.

SK kui Eesti riigi partner väljastab sertifikaate riiklikele isikutele tõendavatele dokumentidele (ID-kaart, elamisluba, digi-ID ja mobiil-ID). Lisaks osutab SK sertifitseerimisteenust elektrooniliste sõidumeerikute projekti raames nii Eestis, Lätis kui ka Leedus. Samuti on SK Leedu mobiiloperaatori Omnitel sertifitseerimisteenuste partner. SK on loonud riigi tellimusena ID-kaardi kasutamiseks vajaliku baastarkvara, sh välja töötanud DigiDoc'i tarkvara, mis võimaldab anda digitaalallkirju, kontrollida digitaalallkirjade kehtivust ning krüpteerida andmeid.

SK on üks juhtivatest eID alal tegutsevatest firmadest Euroopas. MKM on volitanud SKd esindama Eestit mitmetes Euroopa initsiatiivides. Olulisemad neist on usaldusnimekirjade (TSL) ja digitaalse allkirja vormingu arenduste eksperditöö ning teenuste direktiiviga nõutud ühtsete kontaktpunktide elektroonilise andmevahetusega seonduv.

Riigi Infosüsteemide Osakond (RISO), Majandus- ja Kommunikatsiooniministeeriumi Riigi Infosüsteemide Osakond vastutab riigis IKT üldise koordineerimise eest. eID ökosüsteemi osas on RISO spetsiifilised rollid järgmised:

- ametkondadevahelise elektroonse identiteedi alase töögrupi tegevuse korraldamine,
- PKI infrastruktuuri õiguslik reguleerimine,
- järelevalve digitaalsete usaldusteenuste osutajate üle,
- digitaalsete usaldusteenuste registri vastutav töötleja,

- eID infrastruktuuri koosvõime eest vastutav organisatsioon.

Tehnilise Järelevalve Amet (TJA) on digitaalsete usaldusteenuste registri volitatud töötleja. Usaldusteenuste registris registreeritakse kõik Eesti sertifitseerimisteenused ja muud usaldusteenused ja teenuste osutajad. TJA haldab Eesti usaldusteenuste listi EE-TSL ja seostab selle Euroopa usaldusnimekirjade koondnimekirjaga. TJA hindab teiste Euroopa sertifikaate ja hoiab seda väliste usaldusteenuste loetelus VTSL.

Riigi Infosüsteemi Amet (RIA) rollid on:

- digitaalse allkirjastamise infrastruktuuri arendamine ja haldamine,
- struktuurifondide kaudu PKI arendusprojektide korraldamine,
- ID-kaardi baastarkvara arendusprojektide korraldamine,
- PKI lahenduste inkubeerimine.

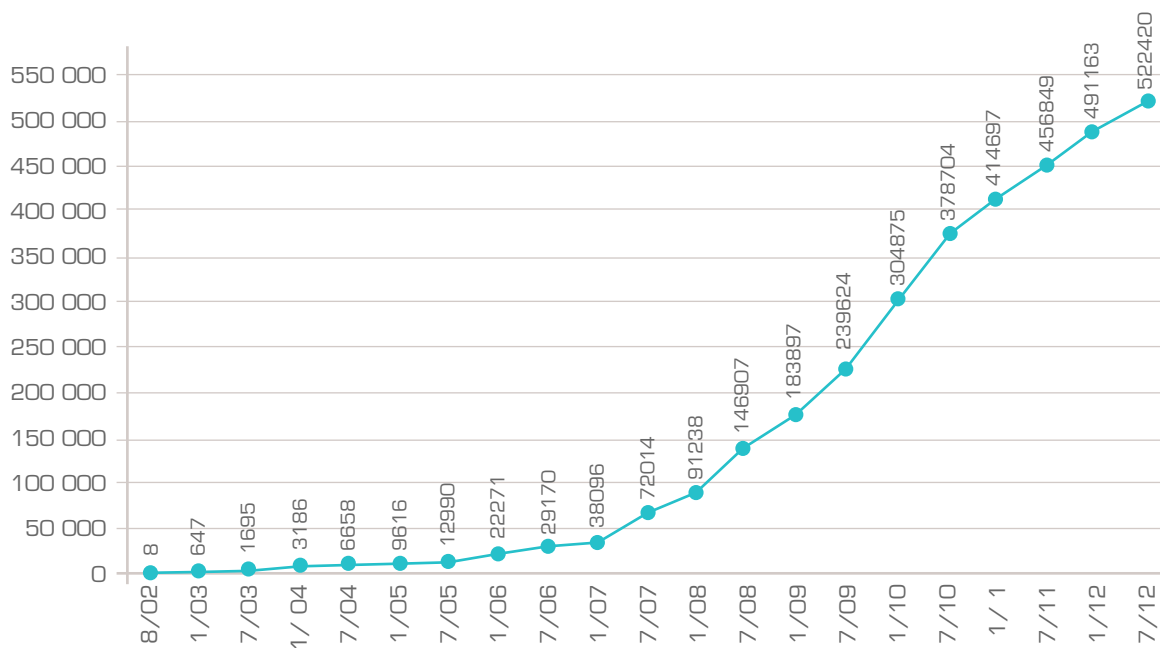
Justiitsministeeriumi Registrate ja Infosüsteemide Keskus (RIK). RIK on üks piirüleste teenuste loomise pioneere Euroopas. E-äriregistri ettevõtjaportaalis saab äriühingu registreerida ID-kaarti kasutades mõne tunniga ja kodust lahkumata. Lisaks äriühingu asutamisele saab ettevõtjaportaali kaudu muuta äriühingu registriandmeid ning esitada elektroonilise majandusaasta aruandeid. Portaal aktsepteerib Soome, Portugali, Belgia ja Leedu ID-kaarte.

Siseministeeriumi Infotehnoloogia- ja Arenduskeskus (SMIT). SMITi kaudu realiseeritakse Siseministeeriumi ja PPA IT-projektid, näiteks süsteemid isikuandmete kontrollimiseks, tagaotsimise andmete sisestamiseks ja edastamiseks Euroopa Schengeni infosüsteemi.

AS Cybernetica. Cybernetica on Euroopa juhtivad turvalahenduste pakkujad. Cybernetica lõi sertifitseerimise registri esimese lahenduse. Tema loodud on riigi infosüsteemide andmevahetuskirgi X-tee sertifitseerimiskeskus. Cybernetica on olnud aastaid ka usaldusteenuste pakkuja. Cybernetica on projekteerinud PKI lahendusi teistele riikidele.

Trüb AG. Trüb trükib Eesti ID-kaarte ja tagab PKI teenused kiibi tasemel.

AS GuardTime. GuardTime on üks Eesti akrediteeritud ajatempliteenuse pakkujatest. Pakub ilma kasutaja võtmata teenust. Avalikus sektoris plaanib selle kasutamist Rahvusarhiiv.



ID-kaardi elektrooniliste kasutajate arv ja juurdekasv august 2002 - juuli 2012

AS Smartlink. Smartlink on avatud platvormi eelistav professionaalne süsteemiintegratsiooni- ja tarkvaraarendusettevõtte. Smartlink on tegelenud ID-kaardi baastarkvara loomisega ja piiriülese kehtivuskinnituse teenuse väljatöötamisega.

Ideelabor. Ideelabor on spetsialiseerunud elektroonilise identiteedi ja sellega seonduvate platvormi-spetsiifiliste probleemide lahendamisele. Koostöös Sertifitseerimiskeskusega on loodud ID-kaardi baastarkvara eri platvormidele. Idee-

labor on spetsialiseerunud OpenID standardil põhinevatele teenustele ja on selle seostanud ID-kaardi ja mobiil-ID infrastruktuuri laiatarbe veebirakendustes.

Kokkuvõtteks: Eesti eID ökosüsteem on loodud ja toimib avaliku sektori ja erasektori koostöös. Eestis on ühtne avaliku võtme infrastruktuur ning eID lahendused on universaalselt kasutatavad, rahuldades ka kõige turvalisemate valdkondade nõudeid.



1 <http://www.sk.ee/kasulikku/digiallkirjastamine>



2 <https://www.niigiteataja.ee/akt/13314840>

Ainulaadne mobiil-ID



HELAR LAASIK

helar.laasik@politsei.ee
Politsei- ja Piirivalveamet

„Eesti on maailmas ka varem silma paistnud innovaatiliste e-lahenduste julge kasutusele võtmisega ning mul on hea meel, et järgmiseks sammuks sellel teel on just mobiil-IDga valimistel osalemine. Läänemaailma demokraatia traditsioonid ja moodne tehnoloogia sobivad omavahel väga hästi.“

Majandus- ja Kommunikatsiooniminister Juhan Parts

Mobiil-ID tõi EMT turule juba 2007. aasta mais ja algselt said seda kasutada vaid ettevõtte oma kliendid. Hiljem hakkasid mobiil-ID teenust pakkuma ka teised operaatorid: Elisa ja Tele2. Teenus osutus kasutajate hulgas ülimalt populaarseks, mobiil-IDga sisselogimist võimaldavate teenusepakujate hulk kasvas kiiresti. Kiire leviku põhjusena toodi enamasti välja kasutajamugavus ja ka vajaduse puudumine ID-kaardi ja selle lugeja järele.

Tekkis olukord, kus käibel oli isiku tõendamiseks tehnilise turvalisuse poolest sobiv vahend, kuid kasutada sai seda ainult väljaspool avalikku sektorit. Populaarsuse kasvuga koos tekkis ka soov tunnustada mobiil-IDd riikliku dokumendina. Ja kui hakkasid lähenema Riigikogu valimised 2011. aasta veebruaris, oligi siht seatud – teha võimalikuks hääletaja autentimine ka mobiil-IDga.

Riiklikku tunnustamist takistas peamiselt kaks asja.

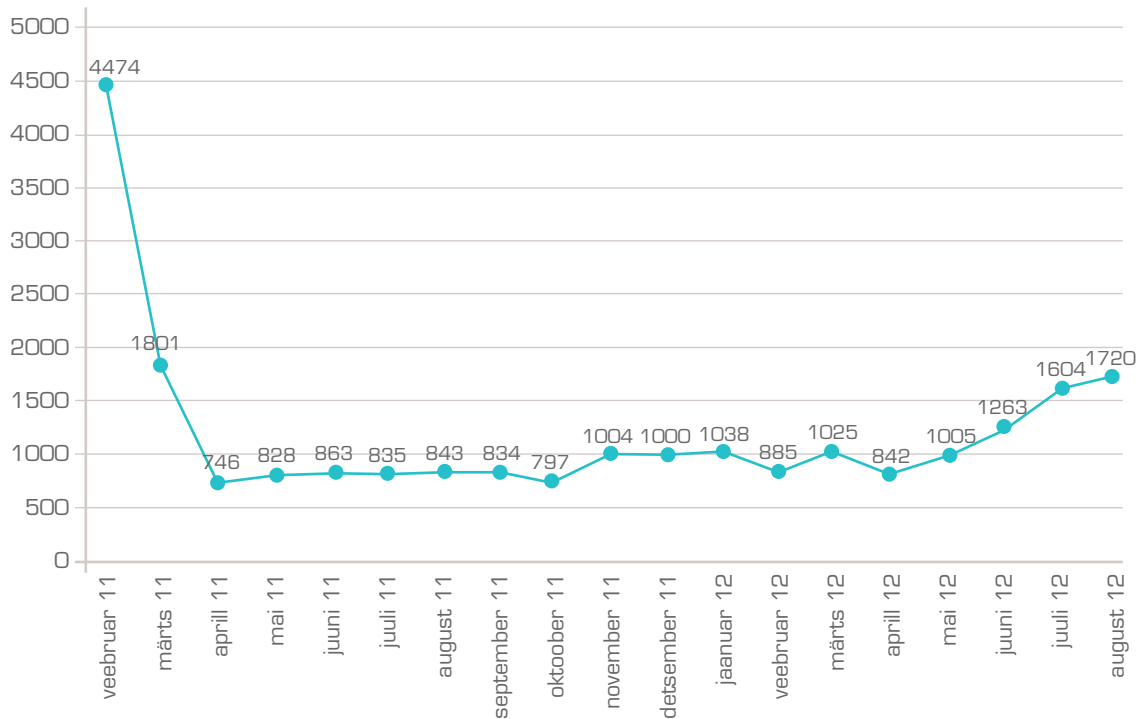
Esiteks ei olnud sellist vahendit Eesti isikut tõendavate dokumentide seaduses – see takistus likvideeriti seaduse 1. jaanuaril 2011 jõustunud redaktsiooniga.

Teiseks anti sellist isiku tõendamise vahendit välja riigi haldusalast väljaspool. Kerkis küsimus,

kuidas saab riik kindel olla, et ta võib võtta vastutuse selle eest, et uus dokument satub ikka õigesti kätte, ja millised riskid siin ees ootavad. Seni oli kasutaja isikusamasuse tuvastamist teinud Politsei- ja Piirivalveameti ametnik, mobiil-ID-võimelisi SIM-kaarte väljastasid kasutajatele aga mobiiltelefonioperaatorid. Inimeste jooksumist mobiiltelefonioperaatori ning Politsei- ja Piirivalveameti klienditeeninduse vahel ei peetud mõeldavaks, seetõttu tuli korrektne isikutuvastamine tagada mobiiltelefonioperaatoritel.

Pärast mitme variandi kaalumist leiti lahendus iseteeninduslikus sertifikaatide aktiveerimises Politsei- ja Piirivalveameti veebikeskkonnas, kuhu sisenetakse ID-kaardiga. Selle lahenduse kasuks sai otsustada tänu nõudele, et isikutunnistuse kasutajatel on kohustus hoida oma dokumenti ja PIN-koode võõraste kätte sattumast. Eeldati, et mobiil-ID sertifikaatide aktiveerija logib taotluskeskkonda sisse ikka oma nime all – selline autentimine on ju piisav näiteks riigiportaalis ja pankades.

Taotluskeskkonda sisenemise järel peab taotleja digiallkirjastama eeltäidetud taotluse (mida ta muuta ei saa) ning kui andmed on korrektsed ja sertifikaadid korras, teeb süsteem positiivse otsuse sertifikaadid aktiveerida. Mobiil-ID on ainus isikut tõendav dokument, kus on võimalik otsus teha inimese osavõtuta. Vea ilmnemisel



Mobiil-ID taotleste arv kuus

protsess peatatakse ning taotleste arv vaatab läbi klienditeenindaja.

Esimesed paar nädalat kulus uue süsteemi töö lihvimisele reaalses keskkonnas, vead aitas kiiresti välja tuua ka juba väljastatud mobiil-ID kaartide suuremahuline aktiveerimine. 2011. aasta aprilliks stabiliseerus taotleste hulk 1000ni kuus ja on siiani jäänud enam-vähem samale tasemele.

Erinevalt ID-kaardi kasutajatest ei tabanud majandusaruannete esitamise tähtaeg mobiil-IDde kasutajaid ootamatult – juunis 2011 taotleste arvu kasvu märgata polnud.

Mobiil-ID näol on e-Eesti saanud endale veel ühe unikaalse isiku autentimise ja digiallkirjastamise vahendi, mida teistes riikides alles hakatakse välja töötama.



Digi-IDst on abi



HELAR LAASIK

helar.laasik@politsei.ee
Politsei- ja Piirivalveamet

Kui digi-ID mõte idanema hakkas, oli Eesti infohiskond jõudnud oma arengus juba sellisele tasemele, kus ilma digitaalse keskkonnata ja ID-kaardita võib aktiivse inimese elu sõna otseses mõttes seisma jääda. Rahaasjade ajamiseks tuleks jälle isiklikult panka minna, linnavalitsusega tuleks silmast silma suhelda, ukсед, kust läbipääsuks on vaja ID-kaarti, enam ei avane jne.

ID-kaarti võib kasutaja seisukohast võrrelda näiteks pesumasina, auto või kas või hadronipõrgutiga – ka see võib vahel puruneda või rikki minna. Eks ole ta ju pisike arvuti, mis kaitsva plastkesta sisse peidetud.

Tuli leida viis, kuidas teha võimalikult lühikeseks aeg, mille jooksul inimene on oma tavapärasest e-maailmast ära lõigatud. Eestis on seadusega määratud, et hiljemalt 30 päeva pärast peab isikul dokument käes olema. Kuid see kuu aega ootamist võrdub mõnes olukorras maakera seisumisega.

Isikutunnistus on turvadokument ja selle tootmine, isikustamine ja logistika peavad vastama paljudele rangetele nõuetele, paraku ei õnnestu aega taotluse esitamisest kuni valmisdokumendi väljastamiseni alla teatud piiri lühendada. Oli vaja mingit muud lahendust.

Tolleaegses Kodakondsus- ja Migratsiooniametis hakati looma lahendust, kuidas isikut tõendavat dokumenti kasutaja nõudmisel kiiresti isikustada. Paraku ei tulnud kõne alla olemasoleva isikutunnistuse isikustamine kohapeal, sest selleks vajalik tehnoloogia on ülikallis ja isikustamine ise peab toimuma ülimalt piiratud ligipääsuga keskkonnas, mida aga üks klienditeenindussaal küll

sugugi ei ole. Seetõttu otsustati luua täiesti uus dokumendiliik, mille sarnast pole praegu maailmas teada – ainult digitaalkeskkonnas toimiv isikut tõendav dokument. Kuna digitaalkeskkonnas on võimalik luua kaardi isikustamiseks turvaline ala, siis elektroonilist dokumenti saab isikustada ka klienditeenindusbüroos.

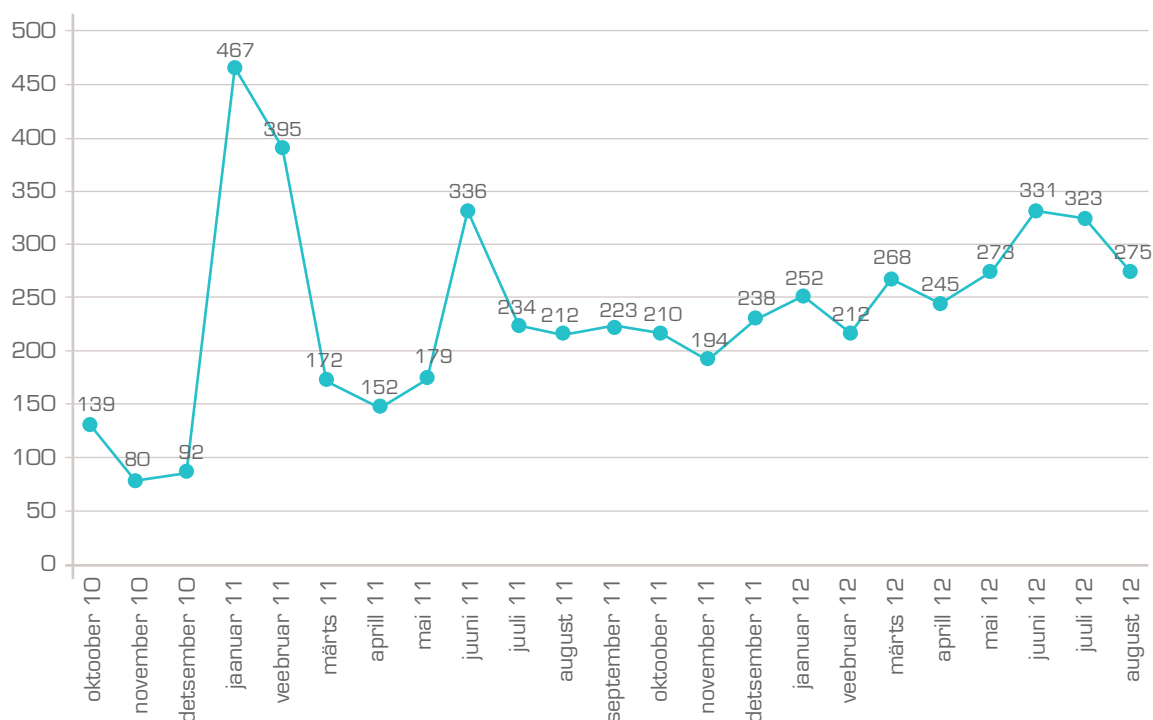
Digi-ID on MultOSi kaart, sellel puudub isikuandmete fail ja tuvastamiseks ning digiallkirja andmiseks vajalik info loetakse kaardil olevatest sertifikaatidest. Sellele dokumendile ei kanta kasutaja näo- ega allkirjakujutist ning seetõttu on visuaalsete andmete kandmiseks võimalik kasutada termosiirdetrükki, mis ei ole nii suure turvalisusega kui lasergraveerimine, kuid ei vaja kalleid isikustamiseseadmeid. Ka on kaardil märges, et seda ei saa kasutada visuaalse isikut tõendava dokumendina.

Esmakordselt tuli nn kiir-ID, nagu seda omal ajal nimetati, kõne alla 2007. aastal, tõsisemalt hakati sellega tegelema 2009. aasta sügisel ja 2010. aasta oktoobris väljastati esimesed 139 digi-IDd.

Uue dokumendi kasutuselevõtmine eeldas muudatusi mitmel alal. Nii tuli välja töötada isikut tõendavate dokumentide seaduse uus redaktsioon ja see Riigikogus vastu võtta. Sertifitseerimiskeskus hoolitses võimaluse eest ühele isikule mitu sertifikaadipaari väljastada ning töötas välja sertifitseerimispoliitika muudatused. Trüb AG tootis kaardid ning seadis need valmis isikustamiseks selleks ajaks juba Politsei- ja Piirivalveameti koosseisu arvatud Kodakondsus- ja Migratsiooniosakonna (KMO) klienditeenindusbüroodes. Politsei- ja Piirivalveameti büroodesse paigaldati



Digi-ID kujundus



Digi-ID taotluste arv kuude lõikes

kaartide isikustamiseks vajalikud printerid, mis saavad hakkama nii kaardile visuaalsete andmete kui ka kiibile elektrooniliste andmete kandmisega. SMIT teostas uue dokumenditüübi ja isikustamisseadmete kasutuselevõttust tingitud muudatused KMO infosüsteemis. Kasutajarakenduste väljatöötajad täiendasid omi süsteeme, et saaks hakata kasutama paralleelseid sertifikaate. Nii et tööd jagus paljudele.

Digi-ID taotluste arv on aina kasvanud. Kui välja arvata 2011. aasta alguses koos uue ID-kaardiga väljastatud digi-IDd, tõusis väljastuste hulk 2011. aasta juunis, kui saabus aeg esitada firmade majandusaasta aruanded. Kuna esma-

kordselt tuli seda teha täisdigitaalselt, selgus nii mõnelegi allkirjaandjale valus asjaolu, et ID-kaart ei tööta ja digiallkirja anda ei saa. Kiireks lahenduseks osutus digi-ID taotlemine, et vajalik toiming sellega ära teha.

Nüüdseks on digi-ID omandanud püsiva koha Eesti isikut tõendavate dokumentide hulgas. Need, kelle isikutunnistus on muutunud kõlbmatuks või kes vajavad täiendavat elektroonilise ja füüsilise funktsionaalsuse kombinatsiooni, mida mobiil-ID ei paku, saavad abi digi-IDst.



Kuidas eID ökosüsteem oma teenuse heaks tööle panna?



URMO KESKEL

urmo.keskel@sk.ee
AS Sertifitseerimiskeskus

ID-kaart ja mobiil-ID on e-Eesti üheks alustalaks ning võimaldanud välja töötada e-teenuseid, mis muidu ei oleks võimalikud. Sageli on aga eID toe lisamisel teenustele kurdetud, et see on tehniliselt keerukas ning põhjustab arendajatele lisatööd.

Kirjeldan siin, kuidas e-teenuse pakkujad saavad oma elu lihtsamaks muuta, eID tehniliste detailidega palju vähem tegeleda ning keskenduda oma teenuse ärifunktsionaalsuse arendamisele. Seda lihtsust võimaldab DigiDocService – SOAP-põhine veebiteenus, mis pakub digitaalallkirjastamise, allkirjade verifitseerimise ning ka eID isikutuvastuse funktsionaalsust.

DigiDocService'i esimene versioon sai avalikuks 2004. aastal ja pakkus ID-kaardiga digitaalallkirjastamise ja DigiDoc-failide käsitlemise funktsionaalsust. DigiDocService toodi turule eesmärgiga pakuda väiksemate ja keskmise suurusega infosüsteemidele senisest lihtsamat võimalust lisada süsteemidele digitaalallkirjastamise tuge. Täna-seks on DigiDocService'i pakutav funktsionaalsus muutunud märksa laiemaks, kui see oli 2004. aastal: DigiDocService'ist on saanud mobiil-ID teenuse üks võtmekomponente ning lisandunud on ka võimalus teenust ID-kaardiga isikutuvastuseks kasutada.

DigiDocService'it pruukivate e-teenuste arv on kasvanud üle paarisaja, mis on märksa enam kui 2004. aastal osati oodata. Seega võib öelda, et DigiDocService'i kontseptsioon on ennast õigustanud.

DigiDocService'i veebiteenus kasutamise peamised eelised võrreldes DigiDoc-teekidega on järgmised.

- DigiDocService'i protokoll on võrreldes DigiDoc-teekidega palju lihtsam.
- Veebiteenus kasutamisel ei ole vaja vaeva näha eri sõltuvustega, mida teekide kasutuselevõtt enamasti põhjustab. Täiendavate süsteemsete ja kolmandate osapoolte teekide paigaldamine pole vajalik, kuna SOAP-tugi on olemas kõikides tänapäevastes arendusraamistiketes.
- DigiDoc-teekides tehtavad parandused, sertifikaatidega seotud muudatused jms on keskselt hallatud – e-teenuse pakkujal ja arendajal on võrreldes teekidega vaja tunduvalt vähem tööd teha uuenduste rakendamisel.

Siiski on olukordi, kus teekide kasutamine on vajalik või eelistatud. DigiDocService ei paku krüp-

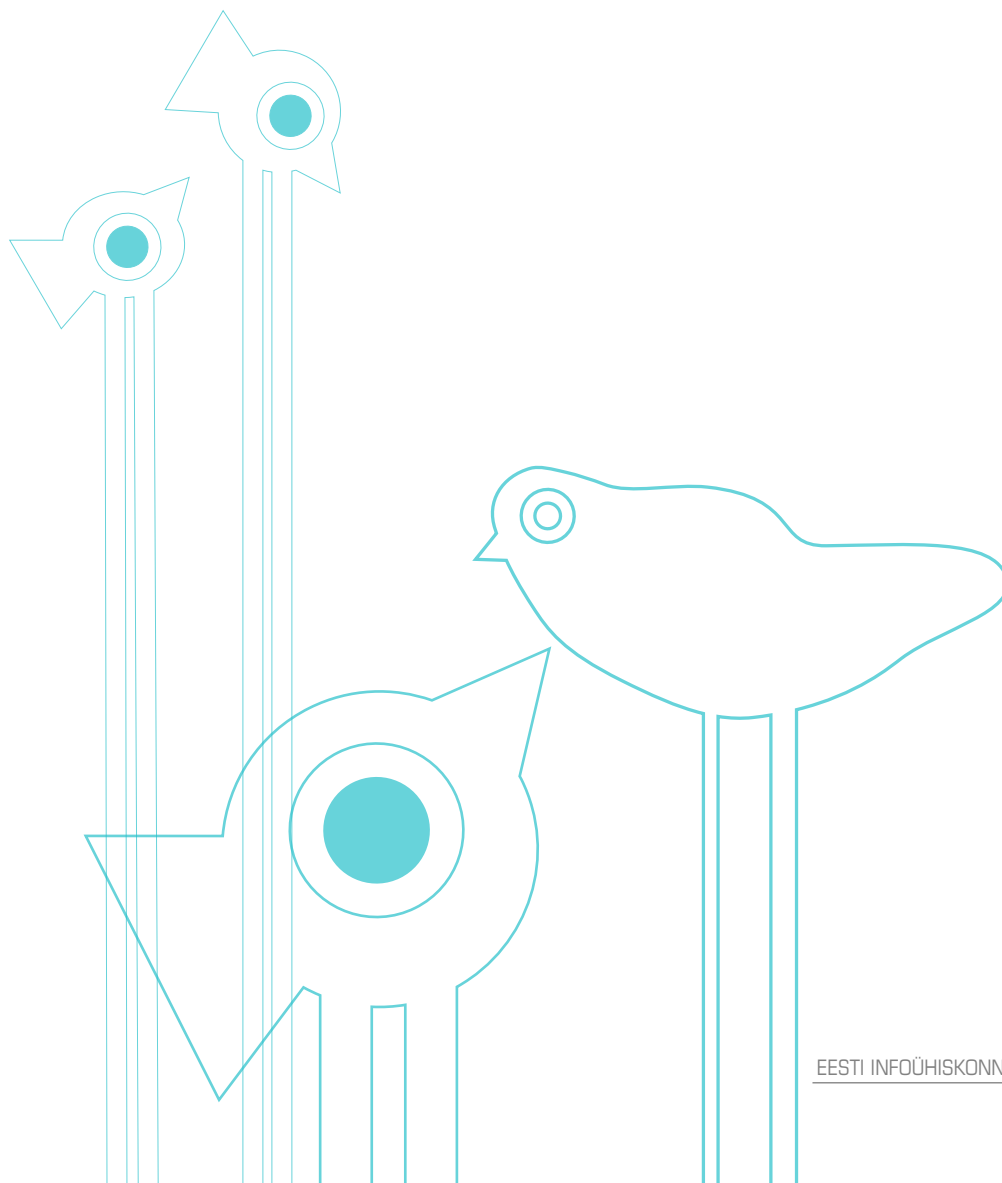
teerimise/dekrüpteerimise funktsionaalsust. Ka väga suurtes mahtudes digitaalallkirjastamise puhul on vahel mõistlikum allkirjastamine teha läbi teekide. Samuti peab DigiDocService'i puhul e-teenuse pakkuja arvestama sellega, et teenusele edastatakse allkirjastatava dokumendi kohta rohkem andmed võrreldes DigiDoc-teekidega digitaalallkirjastamisel.

DigiDocService'it arendades on mõeldud ka sellele, kuidas muuta ID-kaardiga isikutuvastamise toe realiseerimine e-teenuse pakkuja jaoks võimalikult lihtsaks. Isikutuvastamisel on üheks probleemiks olnud see, kuidas sertifikaadis olevad andmed õigesti kodeeringusse teisendada ja kuidas teha sertifikaadi kehtivuse kontrolli, kasutades OCSP teenust. DigiDocService'i teenusele on võimalik edastada isikutuvastuse käigus saadud e-teenusesse siseneja sertifikaat, vastuseks saab teada sertifikaadis sisalduvad isikuandmed ning ka info

sertifikaadi kehtivuse kohta. DigiDocService ise hoolitseb selle eest, et õigest allikast sertifikaadi kehtivust kontrollida ning tagastada sertifikaadis olevad andmed alati samal kujul ja vormingus.

E-teenuste osas Eestis ja Leedus on lisandunud hea uudis. Kui seni oli mobiil-ID funktsionaalsust võimalik kasutada kõikide Eesti mobiilsideoperaatoritega ning Leedu suurima operaatori Omnite-liga, siis 2012. aasta kevadest on lisandunud Leedu mobiilsideoperaatorite Bite ja Tele2 tugi. Lisaks on toetatud ka Leedu ID-kaart. Seega on DigiDocService'i platvormi kaudu võimalik teenindada kõiki Eesti ja Leedu mobiil-ID ja ID-kaardi kasutajaid.

DigiDocService pakub suurepärast võimalust eID arengutega kaasas käia ning e-teenustes ja infosüsteemides eID taristu pakutavaid võimalusi enda äri kasuks tööle panna.



Digitaalne tempel



ANNIKA LJAŠ

annika@sk.ee

AS Sertifitseerimiskeskus

Oleme harjunud, et üks hea ja autentne dokument on asutuse/äriühingu kirjaplangil ja varustatud vastava templiga. Samas on see mõnes mõttes paradoksaalne, kuna tindiga templil ei ole õiguslikku jõudu. Samuti pole teada, kuidas asutuses/äriühingus tagatakse templi kasutamise turvalisus. Digitaalmaailmas on aga võimalik anda templile täiesti uus kvaliteet – digitaalne tempel seotakse tõsikindlalt konkreetse asutuse/äriühinguga. Templi kasutamise eest vastutab antud asutuse/äriühingu juht, kes võib omakorda vastutust delegeerida.

Digitempel tõstab märgatavalt asutuse/äriühingu väljastatava dokumendi usaldusväärust, sest annab selle saajale kindluse, et dokument pärineb just nimelt kõnealusest asutusest. Digitaalset templit ei ole võimalik võltsida. Kui kasutada digitemplit koos digitaalallkirjaga, võib olla veendunud, et allkirja andnud inimene on antud asutusega seotud.

Asutusel/äriühingul saab olla mitme tähendusega digitaalseid templeid, näiteks andmete ja arvete väljastamiseks ning pakkumiste tegemiseks. Üldjuhul kasutatakse digitaalset templit krüptopulgal, millel asub sertifikaadi privaatsõlt ja vastav sertifikaat.

Sertifitseerimiskeskus (SK) väljastab digitempli sertifikaate juba alates 2004. aastast. 2009. aastal reguleeriti digitaalne tempel ka digitaalallkirja seaduses. Digitaalset templit väljastatakse ainult asutustele ja äriühingutele. SK kontrollib enne, kas vastaval asutusel/äriühingul on õigus digitaalset templit saada ja kas templit tellival isikul on õiguslik alus asutust või äriühingut esindada. SK tagab oma siseprotseduuridega, et digitempel jõuaks õige isiku kätte. Kolmandad osapooled, kes saavad vastava juriidilise isiku digitaalse templiga kinnitatud dokumendi, võivad usaldada vastavat dokumenti kui antud juriidilise isiku ametlikku dokumenti.

Digitaalne tembeldamine on lihtne ja käib samamoodi nagu digiallkirja andmine. Tarkvara on ka ühine – DigiDoc. Masstembeldamiseks on loodud tarkvara TempelPlus. Digitempli lahendust on võimalik liidestada enamiku infosüsteemidega ja lisaks saab seda muuta automaatseks. Näiteks kui ettevõtte infosüsteem saadab partneritele automaatseid kirju või teated (arved, saldokinnitused, tellimused jms). Nii ei pea kulutama aega iga dokumendi eraldi tembeldamisele.

Kes juba kasutab digitemplit? Pangad väljastavad digitaalse templiga kinnitatud maksekorralduste kinnitusi, millega tõendatakse makse sooritamist. Tänu sellele on raha saaja kindel, et võib kauba väljastada, kuna raha on reaalset makstud. Samuti on digitempliga kinnitatud kinnisvara hindamisaktid ja liisingfirmade ning pankade edastatavad digitaalsed volikirjad ja lepingud. Aktiivselt kasutab digitemplit ka Riigikantselei, et saata valitsuse otsuseid Riigi Teatajale.

Ehe näide digitempli kasutamise saavutatud ajavõidust ja mugavusest on Eksami- ja Kvalifikatsioonikeskuse, nüüdsest SA Innove, väljastatavad kooli lõputunnistused iga aasta juunis. Varem tuli 40 000 lõputunnistust paberil välja trükkida, vormistada ning postitada, mis võttis aega üle kahe nädala ning oli väga tööjookulukas. Elektrooniline digitempliga lõputunnistus on ka palju turvalisem, sest on võltsimatu ning ajatu õigusliku jõuga.

Eesti on üks vähestest Euroopa riikidest, kes on digitaalse templi seadustanud. Siinse kogemuse vastu tuntakse mujal maailmas suurt huvi. On ülimalt tõenäoline, et digitaalne tempel seadustatakse üle kogu Euroopa praegu menetluses olevas uues e-usaldusteenuste määruses.



Digitaalne allkiri Eestis ja Euroopas – vaade tagasi ja edasi



TARVI MARTENS

tarvi.martens@sk.ee
AS Sertifitseerimiskeskus

Eesti selge liidripositsioon nii Euroopas kui ka kogu maailmas¹ elektroonse identiteedi (eID) valas pole tulnud üllatusena, vaid on kümneaastase sihipärase töö vili. Kui nii mõneski riigis on nagu meilgi ID-kaart kõigile välja jagatud, eristub Eesti siiski selle poolest, et siin neid kaarte elektrooniliselt ka kasutatakse. Pea pool Eesti täisealisest elanikkonnast on vähemalt ühe korra ID-kaarti arvutis kasutanud; üks ID-kaardi või mobiil-ID kasutaja teeb ühes kuus keskmiselt umbes 20 autentimist või digitaalset allkirjastamist.

Ühtne arusaam digitaalallkirjast

Tundub, et Eesti on ainus riik, kus ei vaielda digitaalallkirja vormingu headuse üle ning kus pole põhimõttelisi tehnilisi probleeme nende käsitlemisel. Edu põhjuseks on strateegiavalik – juba 2002. aastal lasti välja hulgaliselt vaba tarkvara nii lõppkasutajatele kui ka süsteemiintegraatoritele. Selle tarkvara kõik komponendid töötlesid sama dokumendivormingut – meile tuttavaks saanud DigiDoc-vormingus ddoc-laiendiga faile. Igaüks eeldab, et tema tekitatud digitaalallkiri on seaduskohane, pikaajalise kehtivusega ning Eestis aktsepteeritud. Ja see eeldus on õige!

Kontrastina on digitaalallkirjade käsitus Euroopas väga kirju ja tihti e-teenusekeskne: ühel hetkel nõuab veebileht inimese käest PIN2 sisestamist ning hiljem lihtsalt tänatakse – digiallkirjastatud tulemit süsteem tagasi ei anna. Paljuski on põhjus selles, et iga e-teenus tekitab digitaalallkirju omas vormingus ja ainult sisemiseks tarbeks.

Ühelt poolt on Euroopa probleemiks 1999. aastal kehtima hakanud elektroonilise allkirja direktiivi käsitusala lõtvus. Eesti seadusandlus nõuab digitaalallkirja koosseisu tõendust, et allkirjastaja sertifikaat allkirjastamise ajal kehtib (muide: sellepärast peamegi olema allkirjastamise ajal internetti ühendatud, et seda tõendust hankida). Direktiiv seda aga ei nõua. Hullempi veel – direktiiv käsib aktsepteerida ka digitaalallkirju, mis on moodustatud palju ebatavalisema vahendiga kui meie ID-kaart või mobiil-ID. See kõik on tekitanud minnalaskmise, mis tähendab, et praktikas vaadeldakse digitaalallkirja pigem kui turvameedet, millel on päris allkirjaga vähe pistmist.

Teiselt poolt on probleemiks digitaalallkirja standardite paljusus ning nende direktiivi jälgendav lõtvus. Populaarseim, ka meil kasutusel olev >>>

» standard XAdES², on nii pikk kui lai, lubades nii eri turvatasemeid kui ka sisemisi tehnikaid ja vorminguid. DigiDoc ei ole muud kui XAdESi konkreetne profiil, mis tagab kõrgeima turvataseme ning viib sisemised valikud miinimumini. Paljud XAdES-ühilduvate tarkvarade tootjad aga toetavad kõiki standardis ette nähtud valikuid, pannes kasutaja keerulise probleemi ette – kuidas üks allkirjastaja võiks teada, milline allkiri selle kontrollijale „meeldib“!?

Eestiga sama teed on läinud Läti (nende XAdESi profiil kannab nime eodc) ja Leedu (adoc). Kahjuks pole aga adoc, edoc ega ddoc ühilduvad. 2007. aastal saavutati Baltic WPKI Forumi töö raames justkui kompromiss – teeme uue profiili nimega BDOC. Eesti on nüüdseks selle adaptee-

rinud rahvusliku standardina, kuid Lätis ja Leedus pole kahjuks selliseid arenguid olnud.

Elu pole aga selles vallas lootusetu. 2012. aasta alul tuli XAdESi standardi hoidja ETSI (European Telecommunication Standards Institute) Euroopa Komisjoni mahitusel välja XAdESi profiiliga³ („Baseline Profile“), mis kitsendab valikuid oluliselt. See on küllalt sarnane BDOCis kirjeldatuga. Standarditud on ka faile ja digitaalallkirju ühendav konteiner ASiC⁴ ja selle profiil⁵, mis klapib meie BDOC standardiga 99%. Need arengud lubavad loota, et liigutakse rahvuslikest standarditest Euroopa standardite poole ning saavutatakse ka digitaalallkirjade koosvõime.

Sinnani on aga veel pikk tee käia. Ka Eestil.



1 <http://www.itif.org/publications/explaining-international-it-application-leadership-electronic-identification-systems>

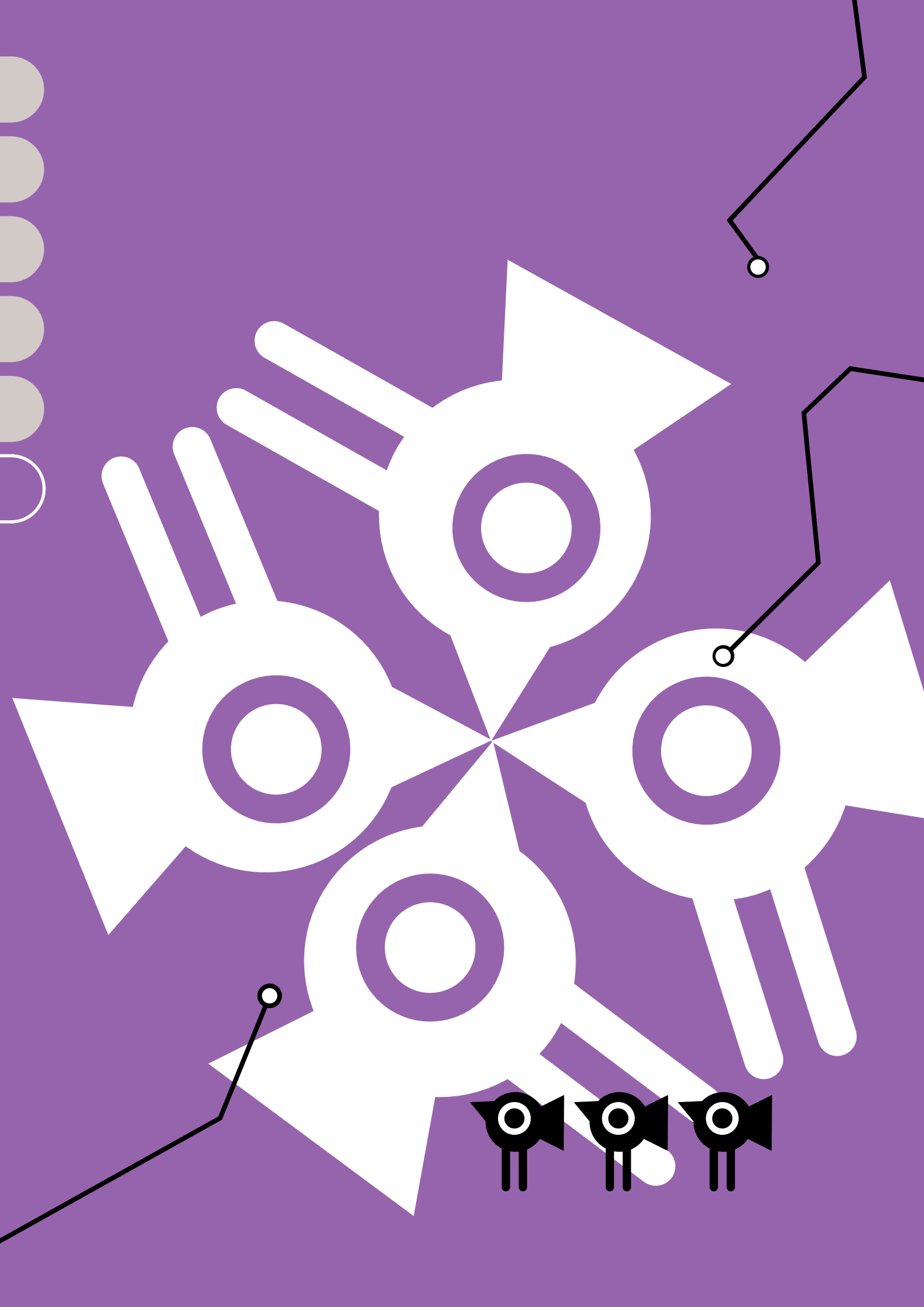
2 ETSI TS 101 903 - XML Advanced Electronic Signatures

3 ETSI TS 103 171 – XAdES Baseline Profile

4 ETSI TS 102 918 – Associated Signature Containers

5 ETSI TS 103 174 – AsiC Baseline Profile





6. PEATÜKK

X-TEE

2011. aasta oli juubeliaasta ühele Eesti e-riigi ja turvalise andmevahetuse alustalale – X-teele. Praeguseks on X-tee jõudnud oma viienda versioonini ning sellega on liitunud üle 100 andmekogu. Seda kasutatakse praegu peaaegu miljon korda päevas. X-tee järjepidevat arengut on varasemates aastaraamatutes korduvalt kajastatud ning selle peatüki avaartiklis heidetakse pilk kogu läbitud teekonnale. Juttu tuleb ka X-tee juurutamiskogemusest teistes riikides, näidates ilmekalt, kui oluline on riigiasutuste koostöö, ühtsete standardite kasutamine ja riigi infosüsteemi loomise põhimõtete reguleerimine. Samuti leiata siit artiklid, mis räägivad ontoloogiate tähtsusest ja kasutusvõimalustest nii e-riigi valdkonnas üldiselt kui ka X-tee teenuste haldamisel ning X-tee viienda versiooni uudsest kodeerimisteenusest.



Esimesed kümme X-tee aastat



AHTO KALJA

ahto.kalja@ria.ee
Tallinna Tehnikaülikool
Riigi Infosüsteemi Amet

X-tee versioonide ajalugu

17. detsembril 2011. aastal sai X-tee kümneaastaseks. Täpsemalt tähendab see seda, et X-tee esimene versioon võeti vastu 2001. aasta 17. detsembril ja oli seejärel kohe valmis vastu võtma X-teega liitujaid, nii andmeandjaid kui ka kasutajaid. Päriselt see kohe nii ei läinud, sest segas paar asjaolu. Esiteks oli ID-kaart veel välja andmata ja tekkis küsimus, kuidas kasutajaid autentida ja autoriseerida. Selleks ajaks olid komertspankadel olemas edukalt toimivad internetipankade lahendused ja tollane RISO juhataja Arvo Ott pidas viljakaid läbirääkimisi suuremate komertspankade asepresidentidega. Lepiti kokku, et pangad võimaldavad oma klientide koodikaarte kasutada lisaks pangateenuste autentimisele ka riigi e-teenuste autentimiseks. Kuid teine mure oli suurem. Nimelt oli tolleaegses andmekogude seaduses kirjas regulatsioon, et kui mingi rakendusülesanne vajab andmeid mitmetest andmekogudest korraka, siis tuleb sellise ülesande lahendamiseks võtta eriluba Andmekaitse Inspeksiost. Ka sellega saadi hakkama, kuid alles sama aasta oktoobris. Seadusesse tehti parandus, et X-tee korral pole sellist eriluba vaja taotleda.

X-tee teise versiooni arendamine algas kohe järgmisel aastal ja valmis täielikult 2003. aasta alguseks. Põhjus, miks uus arendus tehti, oli asjaolu, et 2002. aastal tuli W3C välja uue soovituselise protokolliga SOAP kasutuselevõtmiseks ja seepärast oli mõistlik kohe X-teel üle minna sellele protokollile ja vahetada välja XML-RPC. Hilisem praktika näitas, et see vana protokoll XML-

RPC jäi kasutusele veel mitmeteks aastateks. See jäi kõrvale alles X-tee 5. versiooni tulekuga. SOAP võimaldas paralleelselt kasutada teenuste kirjelduskeelt WSDL ja teenuste repositooriumi standardit UDDI. Need protokollid on praegu kasutusel kogu maailmas ja seetõttu võimaldas õigeaegne üleminek säästa palju arendusraha, sest toimus siis, kui teenuseid oli vähe ja nende ümbertegemise vaev väike.

X-tee kolmas versioon arendati välja aastatel 2003–2004. Kolmandasse versiooni tuli rida uusi täiendusi, mis olid põhjustatud mitmete uute kasutajate vajadustest lähtuvalt. Näiteks seoses Tallinna Linnavalitsuse osakondade (kokku 26) liitumisega oli otstarbekas X-tee juures kasutusele võtta juba nende olemasolev kasutajaõiguste ohjamise süsteem, mis oli välja ehitatud MS Active Directory baasil. X-tee standardne portaal MISP varustati lüüsiga, mis võimaldas MS Active Directory kasutajaõiguste lahendust ära kasutada. Teiseks suuremaks funktsionaalseks muutuseks selle versiooni juures oli asünkroonsete päringute ehk andmeülekannete juurutamine. Aastaks 2003 olid mõned Justiitsministeeriumi kohtute andmeülekanded kasvanud niivõrd mahukaks, et see sadadesse megabaitidesse ulatuv andmevahetus oli mõistlik korraldada asünkroonsel teel. Sellesse versiooni kuulus veel rida pisitäiendusi ja funktsionaalsuse laiendusi, näiteks võeti kasutusele andmekogudest lugemisele lisaks andmekogudesse kirjutamine jne.

X-tee neljas versioon loodi perioodil 2005 kuni 2006. aasta algus. Arendusele eelnes uurimis-

töö, kuidas tõsta andmete salastatust X-teele ja sellega seotud rakendustes. Aastaks 2005 oli vastavalt valitsuse tollasele määrusele kõigil riigiasutustel, mis kasutavad andmevahetust infosüsteemide vahel, kohustus liituda X-teele ja kasutada selle tehnoloogiat. Selgus, et sel ajal käigusoleva X-tee versiooni turvalisus ei vastanud lahendustele, mida vajasisid riigisaladusega seotud asutused, ja seega tuli kasutusele võtta lisatehnoloogiaid andmete krüpteerimiseks. Kui versioon valmis, siis tekkis ka tavakodanikele võimalus korraldada oma andmetöötlust (teenuste kasutamist) nii, et vajadusel krüpteeritakse teenuse kasutamise logid ja lugeda saab kodanik oma logi isiklikul ID-kaardil oleva võtme abil. See versioon oli mitmeid aastaid põhiversiooniks, mille baasil ehitati üles suurte infosüsteemide (e-tervis, Schengeni infosüsteem, e-toimik jne) andmevahetus.

X-tee viies versioon arendati välja 2009 detsember – 2010 oktoober ja seda mitmel põhjusel. Kõigepealt oli X-tee neljas versioon olnud kasutusel juba üle nelja aasta ja päevane teenuste arv üle X-tee oli tõusnud peaaegu suurusjärgu võrra: 2005. aasta 13 miljonilt teenuselt kuni 2009. aasta 100 miljoni teenuseni. Probleemiks polnud niivõrd käideldavus kui asjaolu, et viie aastaga toimub IT arengus palju muutusi ja neid peab jälgima. Näiteks võeti varasemates X-tee versioonides teenuste kirjeldamiseks kasutusele keele WSDL stiil RPC/Encoded, sest seda kasutas enamik infosüsteeme. Aastaks 2009 oli olukord muutunud ja peamine stiil on tänaseks Document/Literal wrapped. Seepärast vahetati välja veebiteenuste kirjeldamise keele stiil. Teine tähtis komponent, mis ajale oli jalgu jäänud, olid krüptoalgoritmid. Oli oht, et Hiina spetsialistid muravad lahti mitmed tuntud algoritmid – seda situatsiooni tuli ennetada. Seepärast vahetati välja X-teele kasutatavad krüptoalgoritmid. Tehnoloogia vahetati uue vastu ka kasutajaliideses. Praegune X-tee Mini-Info-Süsteem-Portaali versioon MISP2 kasutab sama tehnoloogiat kasutajaliidese vormistamiseks nagu ka riigiportaal eesti.ee, nimelt tehnoloogiat Xforms. Üks tähtis funktsionaalsus lisati X-tee 5. versiooni veel. Nimelt on mitmed ministriumid oma andmetöötluses hakanud üle minema andmeaitade kasutamisele. Seejuures on vajalik isikuandmeid töödelda nii, et neid sisaldavatest kirjetest tuleb eemaldada isikut üheselt määravad väljad (nimeväljad, isikukood,

aadress jt). Lihtsam on juba andmete ülekandel andmebaasist andmeaita võtta need väljad välja ja asendada mingi sisu mitteomava koodiga. Sellist operatsiooni toetabki X-tee 5. versiooni sisse ehitatud nn kodeerimisteenus. Loomulikult on viis aastat infotehnoloogias pikk aeg ja selle ajaga tuleb kõrge käideldavusega süsteemist välja palju ebamugavusi ja pisivigu. Ka nende kordategemine oli X-tee 5. versiooni arendamise üks ülesannetest.

X-tee põhilised omadused

Millistele põhiomadustele ja funktsionaalsusele on X-tee tuginenud ja mille arvel on selle kasutavus tõusnud nii kõrgele – peaaegu miljon kasutuskorda päevas?

Kõigepealt hajus arhitektuur. Kui X-teeid projekteeriti, siis oli kohe alguses püstitatud ülesanne, et lahendus peab olema totaalselt hajutatud. Seega tuleb paljuski võtta aluseks samad põhimõtted nagu internetiski, et turvanõudeid silmas

Loomulikult on viis aastat infotehnoloogias pikk aeg ja selle ajaga tuleb kõrge käideldavusega süsteemist välja palju ebamugavusi ja pisivigu. Ka nende kordategemine oli X-tee 5. versiooni arendamise üks ülesannetest.

pidades oleks süsteem laiali paigutatud niipalju kui võimalik. Nii et vältida tuleb selliseid koonduspunkte, mis võiksid pudelikaelaks osutada. Näiteks on mitmed riigid oma andmekogud koonandanud IT-arhitektuuriliselt ühte punkti ehk suurde arvutuskeskusesse. Kui sellise sõlmpunktiga midagi juhtub, siis seisavad tõenäoliselt kõik selle riigi kriitilised teenused. X-tee püüdis juba eos selliseid pudelikaelu vältida.

Siit võib järgmisena esile tõsta X-tee lahenduse teenustepõhisust. Kogu funktsionaalsus on teenustepõhine: X-tee pakub nii riigi infosüsteemi arendamiseks kui ka andmete kasutamiseks teenustepõhist lahendust. X-tee ise kasutab sisemiselt samuti paljusid metateenuseid, mis on teenustena üles ehitatud. Ka tavakasutajatele pakutakse portaalides andmetöötluslahendusi, mis on jälle teenused. Eristatakse elementaarja kompleksteenuseid. Kasutatakse üldtuntuid »»

» teenuste standardeid, nagu SOAP, WSDL, SAWSDL, UDDI jt.

Üks peamisi tähelepanuväärseid X-tee omadusi on kõrge käideldavus. Algusest peale on arendajad ja kasutajad muret tundnud selle üle, kas üle X-tee teostatavad andmetöötlusoperatsioonid pole liiga aeglased ja kas turvaserverid on selleks pudelikaelaks, kuhu palju aega kulub. See pole kindlasti nii. Vastupidi, X-tee üheks ideoloogiks on olnud algusest peale skaleeritavus. Turvaserverite puhul tähendab see seda, et kui teil oma infosüsteemi turvaserveri võimsusest väheks jääb, siis pange asemele suurema tootlikkusega server. Kui see ei aita, tuleb panna mitu turvaserverit paralleelselt tööle ja nende vahel koormust jagada. Kahe paralleelse serveri kasutamine on ka eeliseks selles olukorras, kui üks masinatest juhusliku vea tõttu rivist välja langeb. Võib veel mitmeid X-tee omadusi üles lugeda, nagu logide säilitamine ja nende logide töestusväärtuse tagamine, samuti mitmetasemeline kasutajate autentimine jt.

X-tee statistika, uued suunad, teiste riikide huvi

X-teest rääkides ja kirjutades on alati esile toodud teenuste kasutamise statistikat. Kasutusstatistika on tõusnud juba nii kõrgele kui kuni miljon teenust päevas ja aastas kusagil kuni 240 miljonit teenust. Üha uute infosüsteemide lisandumine X-tee teenuste pakkujate ja nende kasutajate hulka tõstab seda numbrit veelgi.

Mida uut on kavas X-teel? Püüame luua rohkem ja rohkem tööriistu, mis kergendaksid uute

teenuste loomist, teenuste testimist ja nende kasutamise monitoorimist. X-teele on üheks abimeheks riigi infosüsteemi haldussüsteem RIHA, mille abil toimub X-teega liitumine ja mis on endasse kogunud suure hulga andmekogude ja e-teenuste kirjeldusi. Sinna hakatakse edaspidi salvestama näiteks teenuste kvaliteedinäitajaid (ajanäitajad, vigade sagedus jt). Kirjeldused (nt andmeobjektide ontoloogiad) on kasulikud nii selle poolest, et need on inimloetavad, kui ka selle poolest, et need on masinloetavad. Masinloetavus garanteerib selle, et kui asuda olemasolevatest elementaartenustest kokku panema keerulisemaid nn kompleksteenuseid, siis teenuste sisendite ja väljundite omavahelist kokkusobivust saab kontrollida automaatselt. Sellega tegeldakse palju ka teistes riikides ning tihti nimetatakse seda tegevust teenuste komponeerimiseks ja orkestreerimiseks. Me tahame kindlasti teenuste automaatse koostamise juures olla eesrinna ning alustasime koos TTÜ Küberneetika Instituudi teadlastega ühistööd selles valdkonnas.

Lõpetuseks peab ütlema, et X-tee paelub endiselt paljude teiste riikide infotehnoloogide ja infosüsteemide loomise eest vastutajate huvi. Meie arenduspartnerid erafirmad Cybernetica AS ja Aktors OÜ on loonud X-tee sarnase keskkonna Aserbaidžaanile. X-teegea on viimasel ajal aktiivselt käidud tutvumas Venemaalt. Ka naabrid Soomest ja Lätist on külastanud meid. Euroopa Liidu arenguprojektid küsitlevad meid tihti ja peavad tulevaste arengustsenaariumide asjus meiega nõu.



Ontoloogiad ja X-tee teenuste semantiline kirjeldamine



HELE-MAI HAAV

helemai@cs.ioc.ee

TTÜ Küberneetika Instituut

Kaasajal ei piirdu teadmiste vahetus ainult inimestega, vaid sellesse protsessi kaasatakse ka tarkvara agente. Seoses sellega on ontoloogiad (mingi valdkonna mõistete süsteemid) saanud teadmiste semantilise formaliseerimise tavaliseks vahendiks. Selles kontekstis ei vaadelda e-riiki enam kui veebiportaali, kus riigi administratsioon publitseerib kodanikele vajalikku informatsiooni, vaid pigem kui teadmiste vahetamise ja e-teenuste jagamise aktiivset keskkonda, milles üheks osapooleks võib olla tarkvara agent.

Selleks et riigi infosüsteemidesse (IS) kogutud andmetest üheselt aru saada, on vaja ühist tähenduste (mõistete) süsteemi ehk ontoloogiat. Inimesele piisab, kui ISi andmeobjektil on peale tähise ka tekstiline kirjeldus talle arusaadavas loomulikus keeles, tarkvara agent aga vajab tähisest arusaamiseks selle mingit formaalset kirjeldust. Näiteks võib ontoloogiaid formaalselt kirja panna OWLi¹ (Ontology Web Language) keeles. Selleks et nii inimene kui ka tarkvara agent saaksid andmeobjektide tähendusest ühtmoodi aru, on vaja andmeobjektide kirjeldusi laiendada nn semantiliste kirjeldustega ehk viidetega kasutatud mõistetele mingis ontoloogias. X-tee andmeteenused kasutavad ISide andmeobjekte

teenuste sisendi-väljundi parameetritena. X-tee andmeteenuste kirjelduste rikastamine semantiliste viidetega vastavale ISi valdkonna ontoloogia komponentidele annab võimaluse kasutada tarkvara agente ka X-tee andmeteenuste haldamisel.

Ontoloogiade kasutusvõimalused Eesti e-riigis

Ontoloogiatel on palju kasutusalasid nii e-riigi valdkonnas üldiselt kui ka X-tee teenuste haldamisel. Mõned kasutusala on järgmised.

- Informatsiooni ja teenuste semantiline otsing. Ontoloogiad võimaldavad tekitada valdkonnast ühese arusaama ja selle formaalselt esitada. Samuti on valdkonnaontoloogiade abil võimalik seostada eri informatsioonilisi struktuure (nt eri ISide andmeobjekte). Ontoloogiade abil semantiliselt rikastatud informatsioonilisi objekte (nt tekste, pilte, teenuste kirjeldusi, ISide andmeid jms) on võimalik tähenduslikult otsida. Näiteks võib tuua semantilised otsingumootorid Google, Bing jt, mis pakuvad sel otstarbel kasutamiseks portaalis schema.org olevat ontoloogiat veebilehtede annoteerimiseks (nt MicroFormatsi abil). Ka eesti.ee portaali saab valdkonnaontoloogiade olemas-»»

- » olu korral laiendada semantilise (täendusliku) otsinguga. X-tee semantilistelt rikastatud andmeteenuste ja andmeobjektide semantiline otsing on praeguseks RIHAs osaliselt ellu viidud.
- Protsesside disain ja realiseerimine. Paljudel X-tee teenuste pakujatel võib olla suhteliselt sarnane teenuste portfoolio. X-tee teenuste kiiremaks ja kvaliteetsemaks arendamiseks on hea taaskasutada ja jagada teadmisi, selleks sobivad valdkonnaontoloogiad ja nendega rikastatud X-tee teenuste kirjeldused.
 - Koosvõime ja teenuste kompositsioon. Uute X-tee teenuste kiiremaks loomiseks olemasolevatest võib kasutada kompleksteenuste automaatset või poolautomaatset kompositsiooni võimaldavat tarkvara. Selle eelduseks on semantiliselt rikastatud X-tee teenuste kirjeldus. Ontoloogiad saab kasutada ka avaandmete linkimiseks (seostamiseks), tagades sellega lingitud avaandmete kooskõlalisuse.

Riigi infosüsteemide semantilise koosvõime raamistik² näeb ette semantikatehnoloogiate arendamise ja kasutuselevõtu lähimate aastate jooksul. Semantilise koosvõime raamistiku järgi

Ontoloogia loomine võimaldab süsteemiliselt käsitleda valdkonna mõisteid, luues mõistete süsteemi valdkonnast, sellega seonduvast äriprotsessist ja ka vastavast ISi andmekoosseisust.

on iga ministeerium kohustatud looma ning haldama oma valitsemisalaga seotud ontoloogiad, valdkonnasõnastikke ning nendega seotud veebiteenuste semantilisi kirjeldusi. Koosvõime raamistik sätestab OWLi kasutamise ontoloogiate kirjeldamiseks ja SAWSDLi³ kasutamise X-tee teenuste WSDLi kirjelduste semantiliselt rikastamiseks. Riigi andmekogude teenustel baseeruv semantiline koosvõime on eelduseks (või esimeseks etapiks) raamistikus käsitletud üldisemale semantilisele koosvõimele.

Vastavalt RIHA määrusele⁴ on selle andmekogude alamregistrisse kantavate andmekogus töödeldavate andmete koosseisus nõutud lisaks muule ka andmeobjekti semantilise kirjelduse esitamist viitena valdkonna terminile (valdkonna ontoloogia vastavale mõistele, seosele või atri-

buidile). Lisaks sellele tuleb RIHA teenuste alamregistrisse kantavate teenuste andmete koosseisus esitada muu hulgas ka teenuse sisendite ja väljundite semantiline kirjeldus.

Valdkonnaontoloogiate seisust riigis

Nagu eespool mainitud, eeldavad X-tee teenuste semantiliselt kirjeldused ISide valdkonnaontoloogiate olemasolu. Alles nende kättesaadavus teeb võimalikuks X-tee teenuste semantilise kirjeldamise ja ka nende kasutamise mis tahes rakendustes.

Valdkonnaontoloogiate loomiseks on välja töötatud ontoloogiate loomise meetodika⁵ ja ka nõuded RIHAs publitseeritavatele ontoloogiatele⁶.

Peale selle on viimase viie aasta jooksul korraldatud lühemaid ja pikemaid ontoloogiate loomise ja X-tee teenuste semantilise kirjeldamise koolitusi. Aastatel 2010–2011 korraldati koolitused kuuele grupile (igas kuni 12 osalejat) eri ministeeriumide ISide valdkonnast. Need koolitused erinevad varasematest selle poolest, et eesmärgiks oli praktiliselt luua vastav valdkonnaontoloogia ja kasutada seda ka vastava andmekoosseisu ja X-tee andmeteenuste kirjelduste semantiliselt rikastamiseks.

Koolituste tulemusena loodi 2010. aastal 19 ja 2011. aastal 13 ontoloogiat. Põhilised valdkonnad olid seotud RIKi, Rahvastikuregistri, Maaameti, Sotsiaalministeeriumi, e-tervise ja PRIAga. Juba varem kindlaksmääratud X-tee andmeteenuste annoteerimise seisukohast strateegiliselt

tähtsad ontoloogiad on füüsilise isiku andmete, aadressandmete, ruumiandmete ja äriregistri ontoloogiad, mille komponendid katavad umbes 80% praeguste X-tee andmeteenuste sisendi-väljundiparameetritest.

RIHAs on praegu publitseeritud 13 ontoloogiat. See näitab, et mõned koolitustel loodud ontoloogiad pole lõplikult valminud ja publitseeritud. Põhjus on siin mitmeid, kuid põhiline on see, et koolitustest üksi ei piisa töömahuka ontoloogiaarenduse lõpuleviimiseks. Kuna töökohtadel pole selle tegevuse prioriteet kõrge, siis jääb ontoloogiate edasiarendus pärast koolitust soiku. Sellest on muidugi kahju, sest see takistab nende kasutuselevõttu rakendustes ja ka teadmiste jagamist. X-tee teenuste semantilise kirjeldamise seisukohast on tähtis, et peale füüsilise isiku ontoloogia

on ülejäänud kolm strateegiliselt tähtsat ontoloogiat praktiliselt valmis ja ka RIHAs publitseeritud. Füüsilise isiku ontoloogia on valmimisjärgus.

Vaatamata ontoloogiaarenduse teadmisi- ja töömahukusele võib ISI valdaja, arendaja ning haldaja jaoks leida selles tegevuses siiski nii mõndagi kasulikku.

- Ontoloogia loomine võimaldab süstemaatiliselt käsitleda valdkonna mõisteid, luues mõistete süsteemi valdkonnast, sellega seonduvast äriprotsessist ja ka vastavast ISI andmekoosseisust.
- Valdkonnaontoloogia võimaldab valdkonna teadmisi jagada nii teiste ISide ekspertide, mitteekspertide kui ka tarkvara agentidega.
- Eriti kasulik on ontoloogiaarendus uue ISI planeerimisel või vana kaasajastamisel (analüüsi etapis).

ISide kontekstis ei tohi muidugi alahinnata ontoloogiaarenduseks vajalikke ressursse, mis pikaajalisemas perspektiivis tasuvad kindlasti ära.

X-tee andmeteenuste semantilised kirjeldused

Teenuste semantiliseks kirjeldamiseks on loodud juhend⁷, mida kasutati ka ülal nimetatud kooli-

tustel. Kõiki mainitud ontoloogiaid on koolituste käigus kasutatud kas andmekogude või X-tee andmeteenuste semantiliseks kirjeldamiseks. Kahjuks pole praegu RIHAs publitseeritud ühtegi semantiliselt kirjeldatud X-tee andmeteenust ega andmekoosseisu.

Lähemal ajal peaks siiski avalikult kättesaadavaks muutuma aadressandmete ontoloogia abil semantiliselt kirjeldatud vastavate X-tee andmeteenuste kirjeldused.

Kokkuvõtteks

Eesti e-riigi valdkond on tehniliselt valmis rakendada semantilisi tehnoloogiaid, eriti X-tee andmeteenuste haldamise kontekstis. Praegu luuakse X-tee kompleksandmeteenused käsitsi, kuigi semantiliselt kirjeldatud X-tee teenuste korral oleks võimalik seda protsessi osaliselt automatiseerida. X-tee andmeteenuste automaatne või poolautomaatne arendus võiks olla üks võimalikke e-riigi semantikavarade rakendusi riigis.



¹ OWL, www.w3.org/TR/owl-guide

² Riigi infosüsteemide semantilise koosvõime raamistik. <http://www.riso.ee/et/files/RISsemantikaVO7-loplik.pdf>. Versioon 0.7 (01.08.2007).

³ SAWSDL, <http://www.w3.org/TR/sawSDL/>

⁴ Riigi infosüsteemi haldussüsteem. <https://www.riigiteataja.ee/akt/12933746?leiaKehtiv>. Redaktsiooni jõustumise kuup.: 16.02.2009.

⁵ H-M. Haav. Ontoloogiate loomise meetoodika, Tallinn, 2010, <http://ftp.ria.ee/pub/riha/meetoodika.pdf>

⁶ H-M. Haav. Nõuded RIHA ontoloogiatele, Tallinn, 2010, <http://ftp.ria.ee/pub/riha/nouded.pdf>

⁷ P.Küngas. Semantilise kirjeldamise juhend, Tallinn, 2010, http://ftp.ria.ee/pub/riha/Semantilise_kirjeldamise_juhis_v04.pdf

Andmekogude turvaline koondamine



JAN WILLEMSON

janwil@cyber.ee
Cybernetica AS

Andmeid ei koguta mitte niisama, vaid ikka eesmärgiga neid mingi teenuse pakkumisel kasutada. Sageli on vaja andmeid enam kui ühest kogust ning selle mugavaks lahendamiseks ongi Eestis kümnekond aastat X-tee kasutatud.

Kui mingid andmed on kord juba korjatud, võib neist tulu tõusta ka niisuguste ülesandepüstituste puhul, mida algse kogu moodustamisel ette ei osatud näha. Näiteks teadustööde puhul, kui teaduril tekib huvi sotsiaal- või terviseandmete vastu, et uurida eri tegurite mõju rahvastiku käekäigule. Samuti võib niisugustest andmekogudest tõusta tulu riikliku poliitika kujundamisel ja mujal.

Kuid siin kerkib kaks uut probleemi. Paljud andmekogud teadustöö jaoks korjatud ning sel puhul oleks tegemist mitte-eesmärgipärase kasutamisega. Teiseks sisaldavad paljud sotsiaal- ja tervisevaldkonna kogud delikaatseid isikuandmeid, millele teaduril pole õigust ligi pääseda.

Õnneks pole teaduse tegemiseks konkreetsete inimeste identiteet ka vajalik, sest enamasti huvitab meid sedalaadi uuringute korral ainult statistiline lõpptulemus. Küll aga läheb vaja võimalust andmekogusid isikuti seostada. Standardne vahend kirjade seostamiseks on isikukood. Paraku on see aga mingis mõttes liiga võimas, sest peale antud uuringu jaoks vajalike kogude võimaldab ta andmeid siduda ka teiste allikatega ning see võib viia ulatusliku privaatsusriiveni.

Nii on tarvis lahendust, mis tagaks andmekogude seostamise võimaluse ilma identifikaatoreid

(nimesid, isikukode) avamata. Üks meetod on pseudonümiseerimine, st isikukoodide asendamine identifikaatoritega, mida kasutatakse konkreetse agregaatandmekogu moodustamisel.

2011. aasta algul juurutusse läinud X-tee 5. versiooni ongi lisatud mugavad pseudonümiseerimisvahendid. Nn kodeerimisteenus leiab vajalikud pseudonüümid isikukoodide krüptides ning selle teenuse pakkumisel kasutatakse ära X-tees juba olemasolevat turvaserverite taristut. Igasse agregaatandmekogu moodustamisel osaleva allikakogu turvaserverisse paigaldatakse krüptovõti ning X-tee päringuvastustes märgitakse eraldi ära pseudonümiseerimist vajavad väljad. Isiku nimi kustutatakse, krüptitud isikukoodide alusel seotakse kirjed andmekoguks ning tehakse vajalikud statistilised või poliitikauuringud.

Loomulikult ei kindlusta see meid rünnete vastu. Kuna muud väljad peale nimede ja isikukoodide jäävad avatuks, on pahatahtlikul uurijal võimalik mõnede agregaatandmekogusse kuuluvate isikute identiteet teada saada. See tähendab, et liiks kodeerimisteenusele tuleb kasutada ka teisi turvameetmeid, nt nõuda teadurilt oma eesmärkide põhjendamist ning meetodite kirjeldamist. Kui aga uuring on põhjendatud ning väärkasutuse ohtu pole tarvis karta, on X-tee kodeerimisteenus mugav ja efektiivne meetod turvaliste andmekogude moodustamiseks.



X-tee võimalikkusest teises riigis



MONIKA OIT

monika.oit@cyber.ee
Cybernetica AS



ARNE ANSPER

arne.ansper@cyber.ee
Cybernetica AS

Me oleme X-tee üle õigustatult uhked ja tahaksime pakkuda seda kui turvalist ning majanduslikult mõistlikku lahendust ka teistele riikidele infosüsteemidevahelise suhtluse korraldamiseks. Siin on kirjas meie kogemused, nii negatiivsed kui ka positiivsed.

Eeldused

X-tee on turvaline sõnumivahetuskeskkond ning põhimõtteliselt ei takista tööpoolest miski seda kasutusele võtmast mis tahes riigis või ühenduses, kus on vaja lahendada organisatsioonidevahelise infovahetuse probleeme. Ent selleks, et X-tee lahenduse tugevust ja turvaomadusi täielikult ära kasutada, on siiski vaja teatud eeltingimusi.

Oluliseks eelduseks on riigi infosüsteemide koordinaatori olemasolu. X-tee on e-riigi keskne tugisüsteem ning selle haldus nõuab eraldi organisatsiooni, kes peab suutma kõrgete turvanõuetega süsteemi töös hoida ja edasi arendada ning ärgitada riigiasutusi koostööle ja ühiseid

standardeid kasutama. Ent tihti ei ole riikides sellist ministereeriumidevahelist või -ülest usaldatud keskust, kellel ka sobilik võimekus oleks. Oleks mõistlik, kui selline institutsioon oleks loodud enne X-tee juurutamist, sest tegelikult peaks olema kohalik X-tee keskus see, kes kohapeal projekti juhib ning suunab tegevusi juba enne hankeprotsessi. X-tee juurutamine nõuab tugevat selgitustööd väga mitmel tasemel, projekti edukus sõltub suuresti sellest, kui sügavale riikikesse institutsioonidesse see X-tee juurutamise kasulikkuse visioon jõudnud on.

Teine oluline eeldus on võimeka kohaliku partneri olemasolu. See ei ole mingi uudne tõdemus, vaid ammu teada asjaolu, et mis tahes süsteemi juurutamisel mingis teises riigis on võtmeküsimuseks kohalik tugi. Kui me räägime X-teest kui e-riigi põhilisest tugisüsteemist, siis sellise projekti partner peab lisaks valdkondateadlikkusele olema ka poliitiliselt korrektne ja suuteline suhtlema väga kõrgel otsustajate tasemel. Kohaliku keele valdamine on samuti väga oluline. Ühte »»

» kõigi selliste omadustega partnerit ei õnnestugi alati leida, neid peab olema mitu.

Soovid ja võimalused

X-tee juurutamise soov on tekkinud mitmel riigil, näiteks Palestiinal, Moldoval ja Serbial, kus üritatakse leida riigi infosüsteemide ühiskasutusele võimalikult ratsionaalseid lahendusi. Selline soov tekib reeglina siis, kui spetsialistid saavad aru X-tee unikaalsest funktsionaalsusest (unifitseeritud töestusväärtust tagav kõrgkäideldav integratsioonikeskkond) ja poliitikud leiavad viisi X-teeid oma huvides rakendada. Selleks et see soov realiseeruks, on vaja, et ka rahastajatel tekiks tahe X-teeid rahastada. Kui poliitikuid köidavad X-tee toel hõlpsasti realiseeritavad kodanikule suunatud teenused ning spetsialiste X-tee tehnoloogiline väärtus, siis rahastajate veenmiseks pole seni veel võtit leitud.

Kui mingi riigi otsustajad on tööpoolest jõudnud järeldusele, et neil oleks kasulik oma e-riigi rajamisel toetuda X-tee-laadsele lahendusele, siis reeglina tuleb sellise süsteemi hankimiseks teha riigihange. Avalike hangete hea tava ei luba üld-

ja kõikehõlmavaks: kindlasti peab see sisaldama ohtralt riistvara ja muud kasulikuna tunduvat, sest kui ühe süsteemi loomist juba on otsustatud finantseerida, siis üritatakse hankida ühekorruga kõik, mida vähegi annab süsteemi skooopi lisada – mine tea, millal jälle õnnestub. Selline skooopi paisutamine tekitab ebatervet huvi ebaoluliste asjade vastu ja tegelikult olulised teemad (nt süsteemi haldava organisatsiooni ehitamine X-tee puhul) jäävad varju. Nii kipubki otsustavaks saama riistvara pool – kui leidub tarnija, kes näeb tellija ambitsioonikate soovide taga võimalust edasise hoolduse või riistvarauuendustega oma algsed investeeringud tasa saada, võib ta mingi tarkvaralise osa ka oma riistvarale kauba peale kaasa anda. Ja taas on see reeglina tellijale vastupandamatu võimalus.

Õnneks on lisaks paljudele ebaõnnestunud hankekonkurssidele tuua ka positiivseid näiteid. Olgu siin toodud meie kogemus Aserbaidžaani e-riigi loomise projektist, mille raames ühe komponendina realiseeriti ja juurutati ka X-tee tehnoloogial põhinev turvaline infovahetuskeskkond.

X-tee juurutusprotsessi eripära

Väga palju selgitustööd

Kui X-tee juurutamist sisaldav hange on võidetud, siis algab tegelikult järgmine müügiiteratsioon. Ja nagu igal pool mujal, kus uue infosüsteemi juurutamine seniseid protsesse ja harjumusi oluliselt muudab,

tekitab see alguses suurt vastuseisu. X-tee põhimõtted on väga raskelt vastuvõetavad, kuna selle efektiivne juurutamine nõuab mitmete organisatsioonide äriprotsesside koordineeritud muutmist. Kuna enamasti on riigi infosüsteeme üles ehitatud ministriumite vaatevinklist lähtuvalt, siis peavad nende senist elukorraldust puudutavad muudatusettepanekud olema väga oskuslikult põhjendatud ja tulema väga kõrgelt tasemelt, et neid üldse kuulda võetaks.

Siia võiks lisada, et X-tee detsentraliseeritus, andmete mittekoondamine ja juurdepääsukontrolli jätmise seniste omanike kätte on oluline argument tõrkuvate ministriumite veenmiseks. See lihtne lahendus on nii uudne ja üllatav, et selle kommunikeerimine võtab palju aega ja vaeva. Kui ideest aru saadakse, on edasine juba lihtsam.

Me oleme X-tee üle õigustatult uhked ja tahaksime pakkuda seda kui turvalist ning majanduslikult mõistlikku lahendust ka teistele riikidele infosüsteemidevahelise suhtluse korraldamiseks.

juhul riigil hankida X-teeid, vaid turvalist infovahetuskeskkonda, kuigi selle keskkonna funktsionaalsuse kirjeldusega võib hanke objekti ikkagi väga X-tee sarnaseks spetsifitseerida. Aga kui hangitakse infovahetuskeskkonda, siis tegelikult pakuvad selle nimetuse alla kvalifitseeruvaid lahendusi ka mitmed suurfirmad, kel on tagataskust võtta kas firma müügitoetused turule sisenemiseks või oma riigi tugi eksporditoetuste, arenguabi või muu sellise nime all. Ning enamasti eelistavad riigid sel juhul majanduslikult kõige kasulikumat pakkumist, olenemata sellest, kui võrd nõuetekohane see on. Suurfirmad aga näevad selliseid süsteeme kui strateegilisi investeerimisobjekte ja on valmis tegema igasuguseid panuseid, et neid hankeid võita.

Teine tüüpiline nähtus riiklike süsteemide hankimisel on soov teha hange võimalikult suureks

Eestis juurutati X-tee tegelikult jõumeetodil ehk siis valitsuse määrusega, mis esialgu kohustas kõiki riiklike andmekogude andmeid kasutama läbi X-tee. Ei ole mõtet eeldada, et mingis teises riigis saaks see teisiti toimuda. Seetõttu peab X-tee juurutamist toetama mingi sobilik õigusakt, mis teeb selle süsteemi kasutamise riiklikele institutsioonidele kohustuslikuks. Arvestades õigusaktide menetlusprotsessi aeglust, tuleb sellise määruse, ukaasi või muu regulatsiooni eelnõu loomine käivitada vähemalt samal ajal juurutusprojekti algusega. Aserbaidžaanis läks sellise ukaasi kavandist selle kehtestamiseni umbes aasta ja nõudis väga tugevat lobitööd.

Kui selgub, et reguleerimata on ka riigi infosüsteemi(de) loomise üldised põhimõtted, oleks kasulik kohe ka selliste õigusaktide eelnõud välja pakkuda.

Tugisüsteemide tegelik olukord

Teine viivitamatult käivitav teema on kohalike tugisüsteemide tegeliku seisu täpsustamine. Loomulikult oleks hea, kui see pilt oleks olemas juba enne X-tee juurutamise pakkumist, sest hinnang täiendavatele jõupingutustele olemasolevate süsteemide integreerimisel või nendele alternatiivsete lahenduste leidmisel võib muidu olla ebaadekvaatne. Paraku ei pruugi enne lepinguliste suhete algust sellisele informatsioonile ligi pääseda.

Aserbaidžaanis oli näiteks teada, et inimestel on olemas isikukood. Kuid kohapeal selgus, et üleriigilise isikukoodi staatus ja juurutamise mehhanismid on tegelikult kokku leppimata ja kasutusel on mitmed isikuid identifitseerivad kodeerimissüsteemid, millel omavaheline seos puudub. Oli ka teada, et ettevõtetel on olemas „äriregistri“ koodid, kuid paraku selgus, et need on maksuministeeriumi maksumaksjate registri koodid ega ole seotud ettevõtete allkirjaõiguslike isikutega, vaid makse maksvate raamatupidajatega. Selle kogemuse järgi võiks teha julge oletuse, et Eestis, kus on üks isikukood ja üks äriregistrikood, on olukord lihtsalt suurepärane ja see on säästnud riigile palju miljoneid. Väga raske on siduda süsteeme, kui puuduvad võimalused isikute kohta käivate andmete ning isikute-firmade seostamiseks.

Igal juhul tuleb tugisüsteemide osas tehtud eeldusi võimalikult varakult kontrollida, hankides informatsiooni eri allikatest ning tasemetelt, minnes tehniliste detailideni välja. Tuleb ette olukordi, kus juhtkonna arvates mingi teenus toimib, aga spetsialistidelt tulev informatsioon

on täiesti vastupidine. Tuleb saavutada seis, kus kõik osapooled saavad ühtemoodi aru sellest, mis ja kuidas toimib.

Kohalik haldusmeeskond

Kuna X-tee juurutamine eeldab haldusorganisatsiooni loomist ning üsna suuremahulist teadmussiiret, siis on oluline ka personaliteema. Meie õpetund on see, et kohaliku meeskonna loomine ja neile korraliku teadmuse tekitamine ongi kõige olulisem süsteemi edukaks käivitamiseks. Ei maksa loota, et spetsiaalselt selle projekti jaoks on koolitatud või varuks hoiatud sobiliku kvalifikatsiooniga inimesi, pigem tuleb eeldada, et haldusmeeskond tuleb ise luua. Koolitustega tuleb alustada päris baastasemest ja kindlasti ei saa oodata inimestelt ja organisatsioonidelt teadmust ja võimekust, mis on tavapärased Eesti oludes.

Teenuste osutamine

Selleks et mingis teises riigis saaks samamoodi nagu Eestis X-tee teenuseid osutada, peaksid olema paigas üldised põhimõtted andmekogude loomisel. Milliseid andmeid kogutakse, mismoodi, kes vastutab nende õigsuse ja tervikluse eest, kuidas saab infot olemasolevate andmete kohta, et hoiduda andmekogude dubleerimisest jms? Eestis oli selleks algselt andmekogude seadus, praegu on need teemad integreeritud avaliku teabe seadusse. Aserbaidžaanis selliseid seadusi ei ole, riigi põhiregistreid pole määratletud, samuti ka toetavaid süsteeme. Puudub ametlik klassifikaatorite süsteem ning ka maakatastri aluspõhimõtted on kokku leppimata. Samuti puudub aadressandmete süsteem.

Teenuste kasutamine

X-tee põhiline mõte on automaatsete päringute võimaldamises riigi infosüsteemide vahel, ent on selge, et kohe need teenused ei teki, sest need nõuavad mitme osapoole valmisolekut. Kõigepealt saab ikkagi pigem pakkuda mingeid andmete vaatamise teenuseid. Eestiski oli alguses ju põhiliseks teenuseks andmete vaatamise võimalus kodanikele X-tee portaalis, sisukamad teenused tulid hiljem. Esimesed tõsisemad X-tee võimaluste kasutajad Eestis olid politsei ja piirivalve süsteemid.

Aserbaidžaanis huvitab inimesi väga, millist informatsiooni riik nende kohta kogub. Eriti huvitavaks peeti sotsiaalkindlustuse fondi infot, sest inimese pension oleneb summadest, mida tema töödandja on pensionikontole kandnud – seda ei saa aga »»

» inimene ise praegu muul moel teada kui koha-
peale minnes ja küsides. Sotsiaalkindlustuse fon-
di infosüsteem on igati kaasaegne elektrooniline
register ja registripidaja on valmis elektrooniliselt
sellist teenust pakkuma, kui lahendatakse isiku-
koodide teema. Esimeste reaalselt toimivate tee-
nustena pakutakse isiku nime ja aadressi pärin-
gut telefoninumbri järgi ja vastupidi (telefonivõrk
on riiklik ja seda haldab Side- ja IT-ministeerium),
väidetavalt on ka sellisel teenusel kasutajaid.

Siiski võimalik!

Kokkuvõtteks saab öelda, et X-tee tehnoloogiat
on võimalik juurutada ka teistes riikides, aga see

on üsna raske ülesanne. Mitte niivõrd tehniliselt
– kuigi ka süsteemis tuli näiteks Aserbaidžaanis
teha väga olulisi turvataiendusi nende rangema
digitaalalkirja seaduse tõttu –, aga just organi-
satsiooniliselt ja poliitiliselt: see nõuab mitmete
organisatsioonide koostööd ja võib tähendada
riigiasutuste äriprotsesside muutmist. Kuna see
kõik peab tehtud saama juurutusprojekti raames,
siis tuleb arvestada, et see on paras katsumus.





Statistiline ülevaade 2011–2012

Eesti elanike ja ettevõtete info- ja kommunikatsioonitehnoloogia (IKT) kasutamise andmeid kogutakse Euroopa Liidu riikides ühtse metoodika alusel igal aastal. Lisaks põhiandmete kogumisele keskendutakse ka konkreetsele teemale.

2011:

- 16–74aastaste elanike e-oskused;
- ettevõtetes kasutatavd IKT võimalused keskkonnasäästuks.

2012:

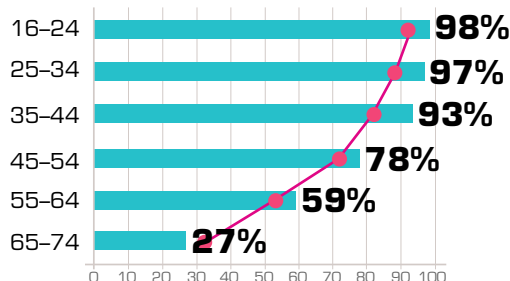
- mobiilse interneti kasutamisharjumused elanike seas;
- e-kaubanduse võimaluste kasutamine ettevõtetes.

Infotehnoloogia kasutamist 16–74-aastaste elanike ja leibkondade hulgas uurib Statistikaamet tööjõu-uuringu lisana alates 2005. aastast, infotehnoloogia kasutamist ettevõtetes aga 2001. aastast¹. Valimisse kuulub 3100 ettevõtet ja üle 4000 Eesti elaniku.

¹ <http://www.stat.ee/49523>

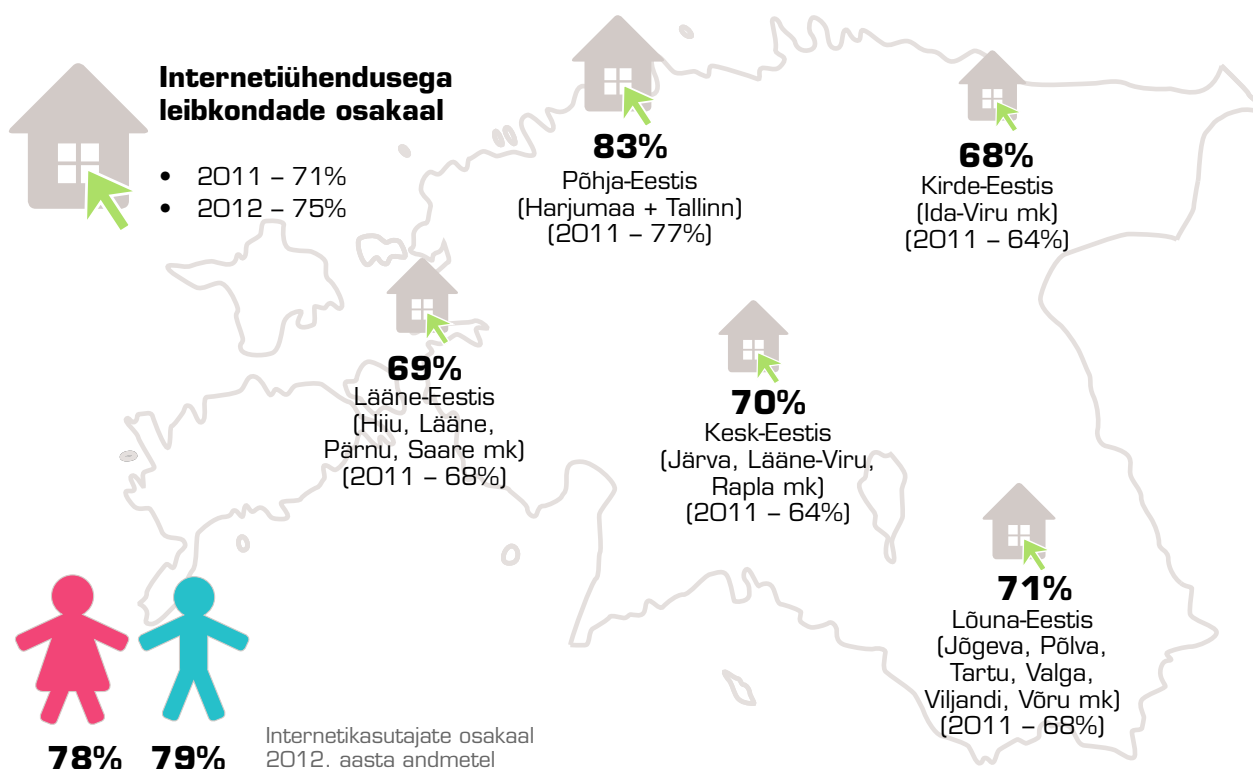
Internetikasutajate osakaal 16–74-aastastest elanikest

- 2011 – 77%
- 2012 – 78%



— Euroopa Liidu keskmine, 2011. aasta andmetel.

Internetikasutajate osakaal Eestis vanusegrupiti 2012. aasta andmetel võrrelduna Euroopa Liidu keskmisega



Infotehnoloogia leibkonnas

Interneti kasutamise eesmärgid

Eesti internetikasutajad kasutavad internetikeskonda väga paljudeks tegevusteks, kuid kõige olulisemad on ikkagi suhtlemine, info otsimine, meelelahutus, samuti internetipank. Kõige populaarsemateks tegevusteks internetis oli 2012. aastal vaieldamatult ajalehtede-ajakirjade lugemine (91% internetikasutajatest; kasv võrreldes 2011. aastaga 3 protsendipunkti), e-kirjade saamine ja saatmine (90%).

Aastaga on märgatavalt kasvanud ka info otsimine toodete ja teenuste kohta. Kui 2011. aastal kasutas seda võimalust 71% internetikasutajatest, siis 2012. aastal juba 89%. Samas ei vii kõik infootsingud e-poodidest ostmiseni. Vaid 30% internetikasutajatest on 2012. aastal interneti kaupade või teenuste ostmiseks kasutanud, naised natuke sagedamini kui mehed. Kõige rohkem ostetakse interneti teel kontserdi-, kino-, teatripileteid jms (48% kõigist e-ostudest). Üle 40% ostetakse e-keskkonnas reisi- ja majutus-teenuseid ning rõivaid ja sporditarbeid. Vähem kasutatakse interneti raamatute, ajakirjade ja e-õppematerjalide ostmiseks (24% e-ostudest). Tasapisi kasvab ka elanikepoolne pakkumine: 2012. aastal kasutas interneti kaupade või teenuste müümiseks ja e-oksjonite pidamiseks 17% internetikasutajatest. Aasta varem oli see 14%.

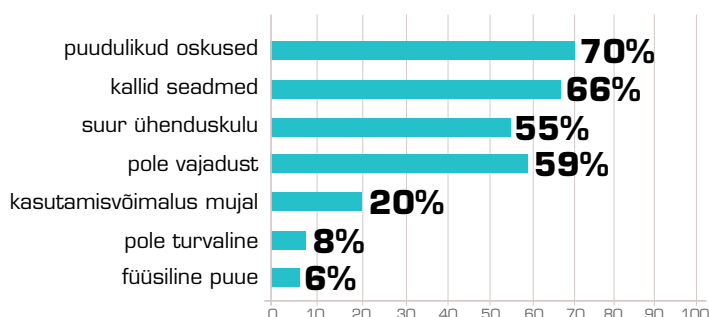
Eraldi paistab silma internetipanganduse kasutamine. Võrreldes 2011. aastaga on siin kasutajate arv püsinud stabiilne: umbes 639 000 kasutajat ehk ligi 90% internetikasutajatest. Euroopas on Eestist internetipanganduse kasutamisel eespool peamiselt Skandinaavia riigid Norra, Island, Soome, Rootsi, Taani, kus ligikaudu 80% kõigist 16–74-aastastest elanikest on internetipanganduse kasutajad.

Väga suurt rolli mängib internet inimeste **suhtlemisvajaduse** rahuldamisel. Nagu mainitud, saadab või võtab vastu e-kirju enamik internetikasutajatest (90%). Üha aktiivsemalt on aga hakatud kasutama interneti helistamiseks või videokonverentside pidamiseks. 2011. aastal kasutas seda võimalust 50% internetikasutajatest, 2012. aastal juba 8 protsendipunkti rohkem. Samuti huvitab inimesi sotsiaalvõrgustikes osalemine (2011. aastal 49% internetikasutajatest) ja teadete postitamine jututubadesse, foorumitesse (2012. aastal 56% internetikasutajatest).

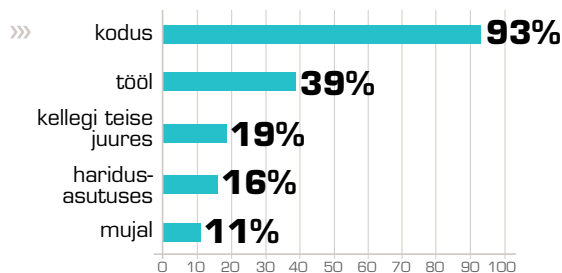
Eesti internetikasutajad armastavad ka internetis pakutavaid meelelahutusvõimalusi. *Online*-mängude mängimise või piltide, filmide, muusika allalaadimisega on tegelenud neist üle poole (56%). Ligi pooled (49%: 2012) internetikasutajatest on kuulnud ka veebiraadiot või vaadanud veebiTV-d. Suhteliselt aktiivselt laaditakse omaloodud digitaalset sisu veebilehtedele teistele jagamiseks (2012. aastal 40% internetikasutajatest). Vähem on neid, kes on loonud oma veebilehe või blogi (12%: 2012).

Mõnevõrra vähem kasutatakse interneti õppimise ja tööelu puhul. Kui vikiidest on infot otsinud üle poole internetikasutajatest (54%: 2011), siis e-kursustel osalemist tunnistas ainult 7,8% (2011). Üle kolmandiku internetikasutajatest on interneti kasutanud ka töö otsimiseks ja töökuulutustele vastamiseks (33%: 2011) ning võrreldes tavaliste sotsiaalvõrgustikega on ametialastes sotsiaalvõrgustikes osalemise määr veel väike, vaid 17% (2011) internetikasutajatest.

Eraldi uuriti 2011. aastal **e-demokraatia** pakutavate võimaluste kasutamist. 23% internetikasutajatest tunnistas, et on kodaniku- või poliitilistel



Joonis1. Internetiühenduse puudumise põhjused 2012. aasta andmetel – osakaal internetiühenduseta leibkondadest



Joonis 2.
Interneti kasutamise koht, osakaal
internetikasutajate seas 2011. aasta andmetel.

teemadel veebilehtedelt lugenud ja ka ise selle teemalisi postitusi teinud. Veelgi aktiivsemad on olnud 11%, kes on nimetatud teemadel *online* aruteludes või hääletamisel osalenud. Euroopas on kõige aktiivsemad e-demokraatia võimaluste kasutajad Soome elanikud, kellest lausa 43% tunnistab, et loeb ja postitab kodaniku- või poliitilistel teemadel veebis.

Majandus- ja Kommunikatsiooniministeeriumi tellimusel küsitakse alates 2011. aastast Statistikaameti andmekogumise käigus Eesti elanikelt ka **avaliku sektori asutuste e-teenuste teadlikkuse, kasutamise ja rahulolu kohta**. Vaid veidi üle 1% (2011, 2012) internetikasutajatest väidab, et nad ei tea ühtegi avaliku sektori asutuse e-teenust.

Kõige sagedamini teatakse ja kasutatakse regulaarselt vajaminevaid e-teenuseid. Tulumaksudeklaratsiooni on e-maksuameti kaudu esitanud 71% (2012) internetikasutajatest ja see osakaal on võrreldes eelmise aastaga kasvanud. Samuti teatakse digiretsepti – võrreldes 2011. aastaga on selle kasutamine kasvanud 13 protsendipunkti (2011: 49% ja 2012: 62% internetikasutajatest). Üle poole internetikasutajatest kasutab ka võimalust tasuta avalike teenuste või riigilõivude eest internetipanga kaudu. Riigiportaali eesti.ee teadlikkus ja kasutamine kasvab tasapisi. 2012. aastal on juba 47% internetikasutajatest selle portaali võimalusi kasutanud.

Samas leidub ka palju e-teenuseid, mida küll teatakse, aga pole kasutatud. Näiteks 2011. aasta valimiste valguses tunnistas 66% internetikasutajatest, et nad teavad e-hääletamise võimalustest. Samuti näitavad kahe aasta võrdlused, et elanikud on teadlikud isikut tõendavate dokumentide taotlemise e-teenusest (2012: 64%), töötukassa e-teenustest (2012: 62%), riigieksamile registreerimise võimalustest (2012: 61%) ja ka näiteks sisseastumisdokumentide esitamise (SAIS) võimalustest (2012: 57%), kuid pole pidanud neid kasutama.

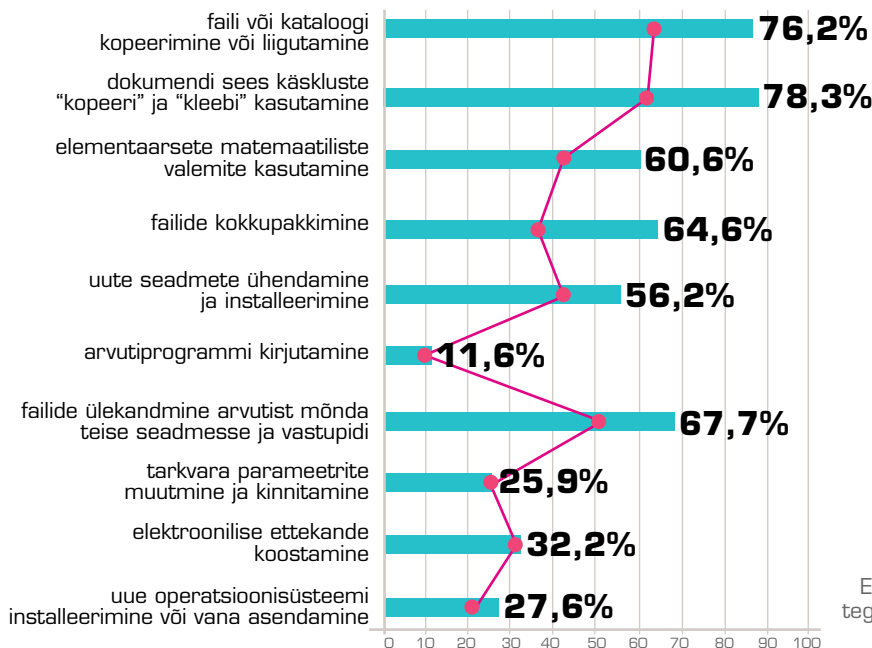
Rahulolu avaliku sektori asutuste e-teenustega on kõrge. 2011. aastal oli avaliku sektori e-teenustega pigem rahul või väga rahul 78% e-teenustest teadlikest elanikest. 2012. aastal oli rahulolevate kasutajate arv tõusnud 81%-ni, kuid väga rahul olevate kasutajate arv vähenes pisut.

16–74-aastaste elanike arvuti- ja interneti kasutamise oskused

2011. aastal koguti detailsemalt andmeid elanike e-oskuste kohta, sest lisaks internetile ligipääsule on üha olulisem teada, mida internetis tehakse. Uuriti, kuidas ja kus arvuti- ja internetikasutamise oskusi omandati, mida arvutiga ja internetis teha osatakse ning kui heaks oma e-oskusi hinnatakse.

Arvuti- ja internetikasutamise **oskuste omandamise** võimalusi on tänapäeval palju. Kui noorem vanuserühm (16–34-aastased) on sageli saanud oma arvuti- ja internetikasutamise oskused juba koolist, siis selle kõrval omandatakse asi väga sageli ka lihtsalt tegevuse käigus. 89% Eesti 16–24-aastastest väidab, et nad omandasid arvuti ja interneti kasutamise oskused koolis. Lisaks väidab kõigist Eesti 16–74-aastasest 72%, et on õppinud e-oskusi tegevuse käigus – enam on see levinud nooremas vanuserühmas. Tegevuse käigus õppimine on populaarne ka Põhja- ja Lõuna-Euroopas: seda on teinud Norras 89%, Rootsis 88%, Soomes 83% kõigist 16–74-aastastest inimestest. Sageli kasutatakse uute e-oskuste omandamiseks ka kolleegide, sugulaste või sõprade abi ning jällegi on nooremates vanuserühmades seda kasutatud ligi 90%.

Märgatavalt vähem käiakse kas siis enda või töödandja initsiatiivil arvuti- ja internetikasutamise täiendkoolitustel. Kõigist 16–74-aastastest on enda algatusel täiendkoolitusel käinud vaid 13%, veidi rohkem 45–55 aastased (22%) ja 35–44-aastased (18%). Samas tuleb mainida, et enda algatusel täiendkoolitustel käimine ei ole eriti populaarne kusagil Euroopas. Aktiivsemad elanikud on Saksamaal (32%), Austrias (21%),



Joonis 3. Eesti elanike arvutiga seotud tegevused võrrelduna Euroopa Liidu (EL 27) keskmisega.

aga näiteks Soomes ja Rootsis ainult 18% kõigist 16–74-aastastest elanikest. Küll aga tuleb võrreldes Põhjamaadega selgelt välja Eesti erinevus tööandja algatusel IT-kursustel käimise osas. Kui Eestis on kõigist 16–74-aastastest elanikest omandanud arvuti- ja internetioskused tööandja initsiatiivil kutsekoolitusel käies 12%, siis Rootsis näiteks 44%, Norras 34%, Soomes 33%. Rootsi 45–64-aastastest elanikest 60% väitab, et nad on just sellisel viisil oma arvuti- ja internetikasutamise oskused omandanud. Eestis on selles vanuserühmas arvuti- ja internetioskusi niimoodi omandanud 16% elanikest.

Arvuti kasutamisega seotud **kursustel mitte-käimise peamiseks põhjuseks** tuuakse piisavaid oskusi – 35% kõigist 16–74-aastastest Eesti elanikest toob välja just selle. Oma oskusi hindab piisavaks üle poole 24–34-aastastest, kuid väga palju ebakindlamad pole ka nooremad või kuni 44-aastased. Sealjuures võib välja tuua, et 54% Eesti 16–74-aastasest peab oma arvuti-oskusi piisavaks, et leida vajadusel aasta jooksul uus töökoht. Samuti hindab 41% 16–74-aastastest oma oskusi piisavaks, et kaitsta oma isiklikku arvutit viiruste ja muude arvutiprobleemide eest, ning 48% hindab oma oskusi piisavateks, et kaitsta oma isikuandmeid. Siinjuures on enesekindlamad just 16–34-aastased.

Kõige paremateks hinnatakse oma arvuti- ja internetioskusi interneti kaudu sugulaste, sõprade ja kolleegidega suhtlemiseks. Vaid 5% kõikidest 16–74-aastastest peab oma oskusi

selleks mittepiisavaks. Kõige enesekindlamad on 16–24-aastased (98%) ja 25–34-aastased (95%). Isegi 65–74-aastasest elanikest 20% hindab seda oma oskust piisavaks, jäädes küll alla Rootsi sama vanusegrupi hinnangutele – 60%. Siinkohal tuleb muidugi arvestada, et Eestis on 65–74-aastaste seas 25% internetikasutajaid, kuid Rootsis 65%.

IT-kursustel mitte-käimise ühe põhjusena paisab Eesti Euroopas välja ka sellega, et kursustel mitte-käimist põhjendatakse vähese arvuti kasutamisega ning seetõttu ka vajaduse puudumisega. Kõikidest 16–74-aastastest Eesti elanikest toob 18% IT-kursustel mitte-käimise põhjuseks vähese arvuti kasutamise. Eestit edestab vaid Sloveenia ja sama põhjus kordub erinevates vanuserühmades.

Kursustel mitteosalemise põhjuseks võib olla ka soov ise teiste käest õppida. Vanuserühmas 35–44 on Eesti elanikud Euroopa kõige suuremad iseõppijad (65% kõigist selleealistest elanikest), järgnevad Norra (65%) ja Läti (62%). Vanemates vanuserühmades Eesti elanike soov ise õppida langeb – kui 45–54-aastaste seas on see 47%, siis 65–74-aastaste seas vaid 20%.

Mobiilne internet

Mobiilse interneti kasutamine liigub tasapisi ka igapäevaellu. 2012. aastal uuriti põhjalikumalt Eesti 16–74-aastaste elanike mobiilse interneti »»

» kasutamise harjumusi ja probleeme. Mobiilse interneti all on siinkohal mõeldud mobiilsidevõrgu või wifi kasutamist süle- või tahvelarvutiga, aga ka mobiil- või nutitelefoniga. Kõige aktiivsemalt kasutatakse mobiilset interneti sülearvutis (40% mobiilse interneti kasutajatest) ja seda teevad eelkõige mittetöötavad (üli)õpilased, naised ja mehed peaaegu võrdselt. Eelistatavaks ühenduse viisiks on sealjuures wifi (27%) ning mobiilsidevõrk 9 protsendipunkti võrra vähem. Mobiilse interneti igapäevaste või peaaegu igapäevaste kasutajate seas on rohkem mehi ja 16–24-aastaseid.

Mobiil- või nutitelefoniga kasutatakse mobiilsidevõrku ja wifi-ühendust peaaegu võrdselt (vastavalt 17% ja 15%). Kui sülearvutiga mobiilse interneti kasutamisel on domineeriv pigem harvem kasutamine (vähem kui üks kord nädalas), siis mobiil- ja nutitelefoni kaudu interneti kasutamisel on valdav igapäevane või peaaegu igapäevane kasutamine. Sealjuures on peamisteks kasutajateks mehed ja võrdselt nii 16–24 kui ka 35–44-aastased elanikud. Harvem kui üks kord nädalas kasutavad mobiil- või nutitelefoni kaudu interneti pigem naised ja 25–33-aastased.

Tahvelarvutiga mobiilse interneti kasutajate osakaal kõigi mobiilse interneti kasutajate seas oli 2012. aastal 7%. Sealjuures mehed ja naised peaaegu võrdselt: mehed 8%, naised 6%.

Mobiilse interneti mittekasutajad toovad peamiseks põhjuseks vajaduse puudumine. 90% mobiilset interneti mittekasutavatest naistest väidab, et neil ei ole vajadust interneti väljaspool kodu ja töökohta kasutada. Samuti toob selle

põhjuse kõige rohkem välja vanusegrupp 35–54. Märnatavalt vähem tuuakse mittekasutamise põhjusena välja teised probleemid, näiteks seadmete ja/või ühenduse kallidus (36% mittekasutajatest) – sel põhjusel mittekasutajad on nimelt hinnatundlikumad: töötud, pensionärid ja mittetöötavad (üli)õpilased. Vanemad vanuserühmad toovad rohkem välja ka selliseid probleeme nagu väikese ekraani ebamugav kasutamine, oskamatuse kasutada või liiga keeruline kasutamine ning ka mure turvalisuse ja privaatsuse pärast.

Mobiilse interneti kasutajate kõige suuremaks probleemiks on pidevad raskused mobiilvõrgu signaaliga (22% kõigist mobiilse interneti kasutajatest). Natuke üle 10% kasutajatest toob välja ka probleemid väikese ekraaniga, internetiühenduse seadete seadistamise ja muutmisega, aga ka ootamatult suuri arveid. Viimastega on hädas eelkõige 16–24-aastased.

Mobiilset interneti kasutatakse eelkõige e-kirjade saatmiseks ja saamiseks (76% mobiilse interneti kasutajatest), uudiste, ajalehtede, ajakirjade jms lugemiseks (63%) ning sotsiaalvõrgustikes osalemiseks (59%). Eelkõige nooremate vanusegruppide tegevuste seas on ka mängude, piltide, filmide, muusika jms mängimine või allalaadimine (kokku 48% mobiilse interneti kasutajatest) ning huvipakkuvate audio- ja videofailide saamine *podcasti* kaudu (24%). *Online* või e-raamatuid loevad ja laevad alla peamiselt 16–24-aastased ja mittetöötavad (üli)õpilased. Väga sageli minnakse pihuseadmega interneti ka tööülesannete täitmiseks. 82% tööga hõivatud internetikasutajatest kasutas pihuseadme abil interneti tööülesannete täitmiseks.

Infotehnoloogia ettevõtteis

Infotehnoloogia kasutamist uurib Statistikaamet alates 2001. aastast. Sealjuures uuritakse nii üldisi arvuti ja interneti kasutamise trende, interneti kasutamist suhtlemisel avaliku sektoriga aga ka ettevõttesiseste protsesside tõhustamist infotehnoloogiliste vahenditega. Statistikaameti valimisse kuuluvad ettevõtted, kus on 10 või rohkem töötajat.

Eesti kõige internetiseeritumad ja arvutiseeritumad ettevõtted on üle 250 töötajaga firmad, kus kõigis on olemas arvutid ja internetiühendus. Samas on ka uuringusse hõlmatud kõige väiksemate, 10–19 töötajaga ettevõtete seas arvutite ja internetiühenduse olemasolu osakaal üle 90%.

Ettevõtte **veebilehe** tähtsust ei ole kolmandik Eesti ettevõtetest enda jaoks veel avastanud. Kui suurtes ettevõtetes (üle 250 töötaja) on veebileht valdavalt olemas, siis väikeettevõtetes on veebileht 66%-l. Oma veebilehel näidatakse kõige rohkem tootekatalooge ja hinnakirju (70% veebi-

lehega ettevõtetest), kuid *online*-tellimise või brooneerimise võimalusi pakub alla 20% veebilehega ettevõtetest. Veelgi vähematel (10% veebilehega ettevõtetest) juhtudel on tellijal võimalik oma teenuse täitmist veebis jälgida. Ligi veerand veebilehega ettevõtetest annab oma kodulehel infot vabade töökohtade kohta või isegi võimaldab *online*'is töökohta taotleda.

Ettevõtte konto mõnes **sotsiaalvõrgustikus** oli 2012. aasta jaanuari seisuga ligi 20% ettevõtetest. Sotsiaalvõrgustike kasutamine on levinud suuremate ettevõtete seas, aga välja saab tuua ka ettevõtted, mis tegelevad hariduse, kunsti, meelelahutuse, vaba aja, info ja side ning majutuse ja toitlustusega. Nende valdkondade ettevõtetest oli sotsiaalvõrgustiku konto olemas üle pooltel.

Lisaks veebilehele on suur-ettevõtete seas rohkem levinud ka **kliendisuhete haldamise tarkvara (CRM)** ja **ressursihaldustarkvara (ERP)** kasutamine. Aastate jooksul on nende tarkvarade kasutamise populaarsus iga-aastaselt paari protsendipunkti võrra kasvanud. Ressursihaldustarkvara kasutab üle poole (53%) suurettevõtetest ning kliendihaldustarkvara 40% suurettevõtetest.

Ettevõtte tegevuse efektiivsemaks muutmisel on üheks võimaluseks kasutada ettevõtte sees, aga ka väliste partneritega suhtlemisel **automaatset andmevahetust**. See on teadete vahetus (näiteks tellimused, arved, maksetehingud või kaupade kirjeldused) ilma neid käsitsi trükkimata interneti või muude arvutivõrkude kaudu automaattöötlust võimaldavas kokkulepitud formaadis. Keskmiselt 37% ettevõtetest kasutas nii 2011. kui 2012. aastal automaatse andmevahetuse võimalusi. Sealjuures on kõige sagedasemaks automaatse andmevahetuse partneriks avalik sektor. Kolmandik ettevõtetest on avalikult sektorilt saanud või saatnud andmeid (maksetagastused, statistilised andmed, impordi või ekspordi deklareerimine jne). Alla veerandi ettevõtetest on kasutanud automaatset andmevahetust ka tooteinfo (tootekataloogid, hinnakirjad) saamiseks või saatmiseks. Saatedokumentide saamine-saatmine ning maksejuhendite saatmine finantsinstitutsioonidele on juba vähem levinud.

Automaatse andmevahetuse partneriteks võivad olla ka ettevõtte eri tegevusüksused, kes

kasutavad ühist tarkvara, andmebaasi või omavahel seotud andmeid. Nii 2011. kui 2012. aasta ettevõtete ankeedis uuriti varude juhtimise üksuse, raamatupidamisosakonna, tootmis- või tarbijateeninduse ja turustusüksuse ligipääsu tellimuste ja ostukorralduste elektroonilisele ja automaatsele infole. Kõige sagedamini on sellisele infole automaatse andmevahetuse kaudu ligipääs raamatupidamisosakondadel (36% arvuteid kasutavatest ettevõtetest). Keskmiselt veerandil arvutit kasutavatest ettevõtetest on loodud automaatse andmevahetuse kaudu ligipääs ka teistele üksustele.

2011. aastal uuriti täpsemalt **avatud lähtekoodiga tarkvara** kasutamist Eesti ettevõtetes.

Ettevõtte tegevuse efektiivsemaks muutmisel on üheks võimaluseks kasutada ettevõtte sees, aga ka väliste partneritega suhtlemisel automaatset andmevahetust.

Kõige rohkem kasutatakse avatud lähtekoodiga internetibrausereid (71% arvuteid kasutavatest ettevõtetest), aga pooled ettevõtetest eelistavad kasutada ka avatud lähtekoodiga kontoritarkvara. Sealjuures kasutavad avatud lähtekoodiga kontoritarkvara kõige vähem suurettevõtted ja kõige rohkem 20–49 töötajaga ettevõtted. Mõnevõrra vähem kasutatakse avatud lähtekoodiga operatsioonisüsteeme (23% arvuteid kasutavatest ettevõtetest), avatud lähtekoodiga veebiservereid (17%) ning avatud lähtekoodiga ressursihaldustarkvara ja kliendihaldustarkvara. **ID-kaardi** kasutamine ettevõtetes näitab pidevat tõusu. Kui 2010. aastal oli ID-kaarti kasutanud 67% ettevõtetest, siis 2012. aastal juba 91%. Sama valdav on ka ID-kaardi kasutamine digiallkirjastamiseks – 2012. aastal tegi seda 89% ning üle poole (67%) ettevõtetest kasutab ID-kaarti kasutajate tuvastamiseks infosüsteemides.

Järjest suuremat majanduskasvu allikat nähakse **avaliku sektori andmete** kasutamises äriilistel eesmärkidel. Siiski kasutab avaliku sektori andmeid äriilistel eesmärkidel olulisel määral umbes 10% ettevõtetest. Samas umbes kolmandik ettevõtetest ei näe selliste andmete äriilisel kasutamisel võimalust. Eelkõige on skeptilised väikesed, 10–19 töötajaga ettevõtted. Teadlikkus avaliku sektori andmete äriilise kasutamise võimalustest on aastaga natukene kasvanud: kui 2011. aas-»

» tal väitis pea 14% ettevõtetest, et ei tea sellisest võimalusest, siis 2012. aastal ei tea sellisest võimalusest 12% internetiühendusega ettevõtetest.

Teine oluline trend on info- ja kommunikatsioonitehnoloogia võimaluste kasutamine keskkonnasäästuks. 2011. aastal uuriti arvuteid kasutavate ettevõtete **keskkonnasäästu tegevusi**. Kõige rohkem (68% arvuteid kasutavatest ettevõtetest) on püütud vähendada paberi kasutamist trükkimiseks ja paljundamiseks. Aga ka pea samaväärselt palju asendatakse isiklik kohaleminek ja reisimine telefoni, veebi või videokonverentsi kaudu suhtlemisega. Üle poole ettevõtetest (59%) on mõelnud info- ja tehnoloogiaseadmete energiatarbimise vähendamisele, kasutades näiteks arvutite ja ekraanide väljalülitamist, automaatselt väljalülituvaid mehhanisme IKT-seadmetes või ka mitmefunktsionaalseid seadmeid – kontorikombaine. Samuti pakutakse töötajatele kaugligipääsu ettevõtte e-postile, dokumentidele, rakendustele. Keskkonnasäästu põhimõtete järgimine on enam levinud suuremates ettevõtetes, kus ka efekt on ilmselt suurem.

Eesti ettevõtete **rahulolu avaliku sektori e-teenustega** on läbi aegade kõrge olnud ning oli seda ka 2011. ja 2012. aastal. Vaid 4% avaliku sektori e-teenuseid kasutanud ettevõtetest ei ole nende teenustega rahul. 2012. aastal kasvas ka nende ettevõtete osakaal, kes on avaliku sektori e-teenustega väga rahul, tõustes 22%-ni. Sealjuures kasutavad pea kõik internetiühendusega ja 10 või enama töötajaga ettevõtted avaliku sektori asutuste e-teenuseid.

Lisaks elanikele mõjutavad **mobiilse interneti** kasutamise võimalused ka ettevõtteid. Peaaegu pooled (48%) Eesti ettevõtetest (sh alates 250 töötajaga ettevõtetest 80%) on pakkunud oma töötajatele tööülesannete täitmiseks mobiilset internetiühenduse kasutamist võimaldavaid sead-

meid (mobiiltelefon, nutitelefoni, netipulgaga sülearvuti jms). Enamasti pakutakse töötajatele tööülesannete täitmiseks süle- või tahvelarvuteid. Valdavalt kasutati neid seadmeid ettevõtte meilüsteemile ligipääsemiseks (87%) või internetis olevale avalikule infole ligipääsemiseks (86%), vähem ka ettevõtte dokumentidele ligipääsemiseks ja nende muutmiseks (57%).

Mobiilse interneti mittekasutamise suurim põhjus on vajaduse puudumine (16% internetiühendusega ettevõtetest), kus kõige vähem tundsid mobiilse interneti järele vajadust 50–99 töötajaga ettevõtted. Samas on takistusteks ka probleemid mobiiltelefonivõrgu internetiühenduse endaga (12%), aga ka tehnilised raskused või suured kulud mobiilse internetiühenduse integreerimisel äritarkvaraga (9%). Takistuseks peetakse ka võimalikku turvariski (8%) või siis oskuste ja teadmiste puudust, lepingulisi takistusi või rasket ümberharjumist uute töömeetoditega (7%). Suured liitumis- või ühenduskulud on probleemiks 7% internetiühendusega ettevõtetest.

E-kaubanduse võimaluste kasutamine on Eesti ettevõtete seas veel vähe levinud. E-kaubandus tähendab, et siduv toodete ja teenuste ostumüügitehing sõlmitakse internetis või muu arvutivõrgu kaudu, kusjuures maksmine või kohaletoimetamine ei pruugi toimuda sama kanali kaudu. Kasutada võidakse müüki ettevõtte veebipoest või veebisaidilt, aga ka automaatse andmevahetuse (EDI)¹ kaudu. Küll ei arvata siia hulka tavaline käsitsi trükitud e-post. 2010. ja 2011. aastal müüs vaid 12% arvutit kasutavatest ettevõtetest oma tooteid või teenuseid veebilehe või automaatse andmevahetuse kaudu. Nende kanalite kaudu ostmine oli veelgi väiksem – 8%. Peamisteks müügi ja ostu turuks on Eesti (9% ettevõtetest). Teistesse Euroopa Liidu riikidesse ja mujale maailma müüb alla 3% Eesti ettevõtetest.



¹ EDI – *electronic data interchange*. Siin mõeldud kui üldine termin äriinfo saatmiseks kokkulepitud automaattöötlust võimaldavas vormingus

