Suomen sähköisen äänestysjärjestelmän vertailua
Euroopan neuvoston sähköisten äänestysjärjestelmien suosituksiin

Electronic Frontier Finland – Effi ry
http://www.effi.org/
3.6.2008
Päivitetty 29.11.2009[1]
Toimittanut Antti Vähä-Sipilä

Yhteenveto

Puhtaasti sähköinen äänestys on ongelmallinen, sillä äänestystuloksen oikeellisuuden varmentaminen on tällaisessa järjestelmässä hyvin vaikeaa. Äänestystulokseen voi vaikuttaa hyvin moni äänestysjärjestelmän osa ja ääntenlaskentaa ei perinteisessä mielessä voida tarkkailla. Äänestystuloksen oikeellisuuteen voi vaikuttaa hyvinkin pieni joukko ihmisiä joko tahattomasti ohjelmointivirheiden kautta tai sitten tahallisesti. Järjestelmän tarkastukset ja auditoinnit koskevat nykyisellään vain osaa järjestelmästä ja niiltäkin osin kansalaisen täytyy luottaa alan erityisammattilaisiin.

Tässä dokumentissa tarkastellaan täyssähköisen äänestysjärjestelmän kelvollisuutta Euroopan neuvoston sähköisen äänestyksen suositusten valossa ja esitetään, miksi täyssähköinen äänestysjärjestelmä, jollainen Suomen sähköäänestyspilotissa on käytössä, ei ole näiden suositusten mukainen.

Electronic Frontier Finland ry (Effi) on perustettu puolustamaan kansalaisten sähköisiä oikeuksia. Tällaisia ovat esim. oikeus sensuroimattomaan viestintään, kohtuullisiin käyttöehtoihin digitaalista sisältöä ostettaessa sekä vapaus kehittää ja julkaista avoimia tietokoneohjelmia. Yhdistys herättää keskustelua ja pyrkii vaikuttamaan muun muassa lainsäädäntöhankkeisiin sananvapaudesta ja tekijänoikeudesta Suomessa ja Euroopassa. Yhdistyksellä on tätä kirjoitettaessa yli 1600 henkilöjäsentä.

[1] Tämä dokumentti julkaistiin alun perin lehdistötiedotteen liitteenä 19.6.2008. Tämä on päivitetty versio, joka on tehty Oikeusministeriön sähköisen äänestyksen kokeilun muistion julkaisun jälkeen. Tekstiä on stilisoitu ja päivitetty vastaamaan englanninkielisen vastaavan raporttimme tekstiä. Tämä versio syrjäyttää aiemman version. Mikäli raportissa on virheellisiä tietoja, korjaamme ne mielellämme. Yhteystiedot löytyvät yhdistyksen verkkosivuilta.

Taustaa

Tämä dokumentti vertailee Suomessa kokeiltua sähköisen äänestyksen järjestelmää Euroopan neuvoston suositukseen Rec(2004)11[2]. Suomenkieliset suositusten käännökset on otettu Oikeusministeriön vaalit.fi –sivuston epävirallisesta käännöksestä[3]. Tiedot Suomen äänestysjärjestelmästä perustuvat Oikeusministeriön toimittamaan materiaaliin[4,5,6]. Oikeusministeriö on pyynnöstä toimittanut myös muita järjestelmää koskevia dokumentteja, mutta se on toistuvasti kieltäytynyt toimittamasta järjestelmän tarkkaa toimintaa ja tietoturvaa koskevia asiakirjoja (ks. Liite 1).

Electronic Frontier Finland ry ilmaisi kiinnostuksensa osallistua sähköisen äänestyksen pilotin auditointiin, jonka suorittajaksi oli valittu Turun yliopisto. Effi tarjosi auditoijiksi kokeneita alan asiantuntijoita. Mahdollinen yhteistyö kariutui siihen, että järjestelmätoimittajat vaativat allekirjoitettavaksi salassapitositoumusta, joka olisi voimakkaasti rajoittanut auditoijien mahdollisuuksia kertoa havainnoistaan[7]. Oikeusministeriö ei yrityksestään huolimatta kyennyt edesauttamaan paremman salassapitositoumuksen syntymistä ja tästä johtuen Effi joutuu raportoimaan järjestelmästä perustuen ainoastaan julkiseen materiaaliin.

Määritelmiä

Tässä dokumentissa "sähköinen äänestys" tarkoittaa äänestyspaikalla tapahtuvaa täyssähköistä äänestystä, jossa ei käytetä äänestäjän varmentamaa paperitulostetta[8]. Suomen sähköisen äänestyksen pilotti on esimerkki tällaisesta järjestelmästä.

---

[2] Council of Europe Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. Euroopan neuvosto, 30.9.2004. https://wcd.coe.int/ViewDoc.jsp?id=778189

[3] Suositus koskien sähköisen äänestyksen laillisia, toiminnallisia ja teknisiä normeja. Epävirallinen käännös. Euroopan neuvosto, 30.9.2004. http://www.vaalit.fi/uploads/sv74q1ff29czyb.doc

[4] Pnyx Compliance with the Council of Europe's Security & Audit Standards on e-Voting. Scytl, joulukuu 2004. http://www.scytl.com/docs/pub/science/Pnyx_Compliance_with_CoE_Standards.pdf

[5] Sähköisen äänestyksen pilotti 2008: Tekninen toteutus ja tietoturvaratkaisut. TietoEnator, 28.2.2008. Vaalit.fi –sivustolla oli tätä kirjoitettaessa vanhempi versio dokumentista.

[6] Sähköisen äänestyksen pilottihanke vuoden 2008 kunnallisvaaleissa. Oikeusministeriön muistio, 30.9.2009. http://www.hare.vn.fi/upload/Asiakirjat/10514/30.9.2009, muistio sähköisestä äänestyksestä.doc

[7] Effin blogi 20.3.2008. http://www.effi.org/blog/2008-03-20-Tapani-Tarvainen.html

[8] Englanniksi täyssähköisestä äänestyksestä käytetään lyhennettä DRE, Direct Recording Electronic.

"Perinteinen äänestys" tarkoittaa Suomessa käytössä olevaa paperiseen äänestyslipukkeeseen perustuvaa äänestystä, sekä vaalipäivänä että ennakkoäänestyksenä.

Tarkoitettaessa jotakin muuta äänestysmallia kuin edellämainittuja tämä on erikseen mainittu.

"Äänestäjän varmentama paperituloste" on äänestyslipuke, joka täytetään koneellisesti mutta tiputetaan paperilla perinteiseen uurnaan sen jälkeen, kun äänestäjä on varmistunut sen oikeellisuudesta[9]. Tämä tuloste ei ole "kuitti".

"Kuitti" on äänestäjän äänestyksestä saama paperinen tai sähköinen kuitti. Edellä mainittu äänestäjän varmentama paperituloste ei ole kuitti, sillä kuitti jää äänestäjälle.

Vertailu suosituksiin

Tässä vertailussa esitetyt vaikuttamismahdollisuudet äänestystuloksiin ovat teoreettisia tai hypoteettisia tilanteita, emmekä väitä, että kukaan pilottihankkeen toimittaja olisi pyrkinyt väärentämään vaalitulosta, tuottanut huonolaatuisia komponentteja tai käyttänyt puutteellisia kehitysmenetelmiä.

Olemme tulkinneet Euroopan Neuvoston suosituksia siten, että niiden tulisi pitää myös teoreettisella tasolla, eli myös tilanteessa, jossa jokin pahantahtoinen taho pyrkisi vaikuttamaan äänestykseen.

On myös tärkeää huomata, että tämän raportin mielipiteet koskettavat sähköisestä äänestysjärjestelmää kokonaisuutena, sisältäen sen hankinnan ja käytön aikaiset toimenpiteet, tai sähköisiä äänestysjärjestelmiä yleisesti. Sähköinen äänestysjärjestelmä on yhtä vahva kuin sen heikoin lenkki. Yksittäinen hyvä järjestelmän osa ei pysty takaamaan koko järjestelmän toimintaa. Emme ota kantaa yksittäisten järjestelmän osien vaatimustenmukaisuuteen tai järjestelmätoimittajiin.

Euroopan neuvoston suositusten teksti on tässä dokumentissa kursivoitu.

> *Sähköisen äänestysjärjestelmän toteutuksen on perustuttava laajaan riskikartoitukseen, jossa on arvioitu vaalin tai kansanäänestyksen toimittamiseen liittyviä riskejä. Sähköisessä järjestelmässä on oltava turvatoimia, joiden avulla riskikartoituksessa tunnistetut riskit voidaan välttää.*

Effi toivoo, että tällainen riskikartoitus (tietoturvauhka-analyysi) on todellakin tehty. Sellaisen tuloksia ei kuitenkaan ole Oikeusministeriöstä luovutettu, vaikka sitä on erikseen pyydetty.

Sähköisen äänestyksen pilottia varten Eduskunta sääti väliaikaisen lain. Hallituksen esitys[10] ei viitannut täyssähköisten äänestysjärjestlmien erityisiin riskeihin, vaikka ne

---

[9] Englanniksi äänestäjän varmentamasta paperitulosteesta käytetään termejä (englanniksi VVPT, VVPR tai VVPB, Voter Verified Paper Trail / Record / Ballot).

[10] Hallituksen esitys HE 14/2006. http://www.finlex.fi/fi/esitykset/he/2006/20060014

tunnettiin tuossa vaiheessa hyvin esimerkiksi Yhdysvalloissa. Kaikkein seikkaperäisin ennen vaaleja julkaistu riskianalyysi näyttää olevan muistio[11], joka huomauttaa merkittävästä riippuvuudesta tietotekniikasta ja mahdollisista ohjelmisto-ongelmista, sekä siitä, ettei uudelleenlaskentaa varten ole fyysisiä äänestyslippuja.

Onkin siis hyvin kiinnostavaa, onko yksityiskohtaista, koko järjestelmän kattavaa täyssähköisen äänestyksen riskit huomioon ottavaa riskianalyysiä koskaan tehty.

Oikeusministeriön kieltäytyminen riskianalyysien tulosten antamisesta vietiin korkeimpaan hallinto-oikeuteen yksityishenkilön toimesta[12]. Tätä kirjoitettaessa päätöstä ei ole saatu, mutta lausunnossaan[13] Oikeusministeriö viittasi kahteen dokumenttiin[14,15], joissa saattaa olla riskianalyysitietoja. Ainoastaan toinen niistä on kirjoitettu projektin alussa. Toisen päiväys antaa aiheen olettaa, että se on Turun yliopiston auditointiraportin tavoin kirjoitettu kun järjestelmä on jo ollut lähes valmis.

Effi huomauttaa, että riskikartoituksen tekeminen ohjelmistoista kuuluu nykyään useiden ohjelmistotalojen toimintaan, ja riskikartoitus tulisi tehdä *ennen* toteutusta. Esimerkiksi Microsoft on julkaissut omista menettelytavoistaan jopa kirjan[16]. Mitä todennäköisimmin yksittäiset järjestelmän komponentit on arvioitu toimittajien toimesta, mutta jos koko järjestelmälle ei ole tehty järjestelmätason turvallisuus- ja riskianalyysiä, kyseessä on mielestämme erittäin vakava puute.

> *20. Jäsenvaltioiden on tarpeellisin toimenpitein varmistettava, että äänestäjät ymmärtävät miten sähköinen järjestelmä toimii ja luottavat sen toimintaan* (engl. *understand and have confidence in the e-voting system*).

Aiemmin suosituksessa on todettu, että "*[s]ähköisen äänestyksen tulee olla yhtä luotettavaa ja turvallista* (engl. *reliable and secure*) *kuin äänestys sellaisissa demokraattisissa vaaleissa tai kansanäänestyksissä, joissa sähköisiä äänestysmahdollisuuksia ei käytetä*". Perinteisen äänestelmän luotettavuus (reliability) riippuu hyvin paljolti siitä, että äänestäjät ja toimitsijat ymmärtävät, miten äänestys toimii. Tällöin he osaavat itse havaita mahdolliset luottamusta heikentävät poikkeamat. Sähköisestä järjestelmästäkin tulisi täten olla vastaava ymmärrys.

---

[11] Oikeusministeriön muistio 12.1.2004.
http://www.vaalit.fi/uploads/wtethk6kup41.pdf

[12] Korkeimman hallinto-oikeuden d:no 1683/1/08.

[13] Oikeusministeriön lausunto 20/51/2008, 18.6.2008.

[14] Auditoijan opas. 25.2.2008. Ei julkaistu. Samaan dokumenttiin viitataan myös Turun yliopiston auditointiraportin viiteluettelossa.

[15] Ehdotukset pilotin tuotannonaikaisista toimenpiteistä. 3.10.2006. Ei julkaistu.

[16] M. Howard ja S. Lipner. SDL: The Security Development Lifecycle. Microsoft Press, 2006.

Vastaavan ymmärryksen tason saavuttaminen on kuitenkin tällä hetkellä mahdotonta, sillä ensinnäkin Oikeusministeriö on kieltäytynyt antamasta kansalaisten (ts. äänestäjien) vaatimia tarkkoja tietoja äänestysjärjestelmästä (tämä sotii myös suosituksen 21 henkeä, vaikkakaan ei kirjainta, vastaan: "*[t]ietoa sähköisen äänestysjärjestelmän toiminnasta on oltava julkisesti saatavilla*"). Oikeusministeriön perustelut tietojen antamisen esteille löytyvät liitteestä 1. Ne liittyvät sekä turvallisuustoimenpiteiden salassapitoon että järjestelmätoimittajan liikesalaisuuksien suojaamiseen.

Toisekseen, perinteisen äänestysjärjestelmän ymmärtäminen on mahdollista kenelle tahansa, sillä se toimii fyysisessä paperin, kirjekuorten, puulaatikoiden ja fyysisen turvallisuuden (mm. lukkojen ja ovien) maailmassa. Vastaavalle tasolle pääseminen sähköisen äänestyksen ymmärtämisessä vaatii huomattavia tietotekniikan ja tietoturvan osaamistaitoja, ja tätä ongelmaa heijasteltiin myös ministeriön pilotin kokemuksia käsittelevässä raportissa. Oikeusministeriön ennen äänestystä luovuttamat asiakirjat[17] ovat niin yleisluontoisia, etteivät ne mahdollista vastaavaa ymmärryksen tasoa edes ohjelmistotekniikan asiantuntijoille. Täyden ymmärryksen saavuttamiseksi tulisi saada näkyvyys järjestelmän lähdekoodiin ja ohjelmistokehitysprosesseihin.

Tämän vuoksi kansalaisten enemmistön täytyykin luottaa kolmanteen osapuoleen, joka katselmoi (auditoi) sähköisen järjestelmän ja antaa siitä lausuntonsa. Verrattuna perinteiseen äänestykseen luottamus tiivistyy huomattavasti pienempään joukkoon ja ymmärrys ei todellisuudessa koskaan ole samalla tasolla kuin perinteisessä äänestyksessä.

Sen lisäksi, että kansalaisen tulee luottaa pieneen auditoijien joukkoon, tässä nimenomaisessa tapauksessa järjestelmän auditoijatkin ovat mitä todennäköisimmin salassapitositoumuksen alaisuudessa. Tämä voi rajoittaa sitä, kuinka paljon he voivat löydöksistään kertoa.

Effi ymmärtää liikesalaisuuksien tarpeen kilpaillulla alalla. Kuitenkin, kun kyseessä on demokratian perusteisiin kuuluva äänestysjärjestelmä, Oikeusministeriön päätös valita salassapitositoumuksin ja liikesalaisuuksin suojattu ratkaisu sotii mielestämme Euroopan neuvoston vaatimuksen henkeä vastaan.

> *23. Kaikkien tarkkailijoiden on lain sallimissa rajoissa voitava olla läsnä tarkkailemassa ja kommentoimassa sähköistä vaalitoimitusta ja myös tulosten laskentaa.*

sekä

> *56. Toimivaltaisen vaaliviranomaisen edustajien on voitava osallistua äänten laskentaan ja tarkkailijoiden voitava tarkkailla ääntenlaskua.*

---

[17] Oikeusministeriö teki huomattavan määrän tietoisuuden kasvattamistyötä verkkosivustonsa http://www.vaalit.fi/ kautta. Valitettavasti siellä julkaistu materiaali on todellisen ymmärryksen saavuttamisen osalta liian yleisluontoista.

Tulosten laskentaa ei sähköisessä äänestyksessä voi perinteisesti ajateltuna suoraan "tarkkailla", sillä äänten laskenta tapahtuu laskentatyöaseman ohjelmistossa. Ohjelmiston käyttäytymistä ei voi ihmisaistein havaita. Ainoat asiat, joita ohjelmiston käyttäytymisestä esimerkiksi silmin havaita ovat ne, jotka ohjelmisto päättää tarkkailijalle näyttää. Se, että tarkkailija näkee jotakin esimerkiksi työaseman ruudulla tai tulostimessa ovat vain välillisiä tietoja laskennan todellisesta tilasta ja etenemisestä. Perinteisessä äänestyksessä laskennan todellista tapahtumista taas voidaan seurata, koska äänestyslipukkeet ovat fyysisiä ja niihin kirjoitetut numerot silmin havaittavissa.

Käytännössä tarkkailijat siis joutuvat luottamaan järjestelmän kehittäjien ja auditoijien kunniasanaan. Tarkkailijat ovat toki tarpeen laskentaryhmän valvonnan vuoksi, mutta itse vaalituloksen laskentaa he eivät pysty tarkkailemaan.

> *25. Ennen kuin sähköinen äänestysjärjestelmä otetaan käyttöön ja sopivin väliajoin sen jälkeenkin sekä erityisesti silloin, kun järjestelmään tehdään muutoksia, on vaaliviranomaisen nimittämän riippumattoman elimen varmistettava, että sähköinen äänestysjärjestelmä toimii asianmukaisesti ja että kaikki tarvittavat turvatoimenpiteet on tehty.*

Kun ohjelmistoja kehitetään, muutokset niihin tehdään nk. lähdekoodiin. Lähdekoodi on ihmisen ymmärtämää ja kirjoittamaa ohjelmaa, joka muutetaan myöhemmin tietokoneen ajamaksi ohjelmaksi.

Lähdekoodi on monimutkaisessa järjestelmässä hyvin iso määrä tekstiä. Se säilytetään tyypillisesti keskitetyssä paikassa, johon ohjelmiston kirjoittajat tuovat tekemänsä muutokset.

Jotta muutoksia voitaisiin todellisuudessa seurata, vaatimuksessa mainitun riippumattoman elimen pitäisi tarkkailla myös tätä ohjelmiston kehityksen aikaa eikä pelkästään valmista tuotetta. Mahdollisten ongelmien löytäminen lopputuotteesta vastaa neulan etsimistä heinäsuovasta.

Suosituksen määrittelemät "tarvittavat turvatoimenpiteet" liittyvät myös siihen, että ohjelmisto on kirjoitettu tietoturvallisuus huomioiden. Tämän vuoksi ohjelmistotoimittajan ja järjestelmäintegraattorin pitäisi saattaa kaikki ohjelmiston kirjoittamisen aikaiset toimintatapansa näkyviksi, esimerkiksi sen, millä tavoin kontrolloidaan, ketkä voivat tehdä muutoksia mihinkin lähdekoodin osaan.

Nämä toimintatavat tulisi myös tehokkaasti varmistaa, jotta voitaisiin varmistua niiden noudattamisesta kaikissa olosuhteissa, kuten sisäisen tai ulkoisen poliittisen painostuksen alla.

> *26. Sähköisessä äänestysjärjestelmässä on oltava mahdollisuus äänten uudelleenlaskentaan. Muut sähköisen äänestysjärjestelmän ominaisuudet, jotka voivat vaikuttaa tuloksen oikeellisuuteen, on oltava todennettavissa.*

Uudelleenlaskennan ajatus on, että laskennassa voi olla muuttuvia ilmiöitä kuten inhimillisiä virheitä, jotka voidaan havaita laskemalla äänet uudelleen ja vertaamalla niitä edelliseen tulokseen. Sähköisessä äänestyksessä uudelleenlaskennan suorittaa

sama laskentatyöasema, joka suoritti alkuperäisenkin laskennan. Ohjelmistot ovat deterministisiä, ts. ne suorittavat samoilla lähtötiedoilla aina samat toimenpiteet. Uudelleenlaskennalla samalla järjestelmällä päädytään samoilla lähtötiedoilla aina samaan lopputulokseen.

Laskettuun tulokseen vaikuttaa myös alkuperäinen äänestysohjelmisto. Mikäli äänten antamisessa ja tallennuksessa on tapahtunut virhe, ei mikään määrä uudelleenlaskentaa - edes riippumattomalla järjestelmällä - pysty pelastamaan tulosta oikeaksi.

Ainoa tapa suorittaa uudelleenlaskenta sähköisessä äänestyksessä on ottaa mukaan jokin järjestelmästä riippumaton laskentamenetelmä. Tällaisia voisivat olla jokin sopiva matemaattinen protokolla, joka mahdollistaisi äänen perillemenon ja oikein laskennan varmistamisen ilman, että äänen sisältö paljastuu, tai äänestäjän varmentama paperituloste, joka pudotetaan perinteiseen uurnaan.

> *32. Järjestelmän keskeisen infrastruktuurin, palvelimien ja vaalitietojen tulee olla ainoastaan vaaliviranomaisen nimittämien henkilöiden käytettävissä. Käytön osalta on laadittava selkeät säännöt. Kriittiset tekniset toimet on suoritettava vähintään kahden henkilön muodostamissa työryhmissä. Työryhmien kokoonpanoa on säännöllisesti muutettava. Mahdollisuuksien mukaan nämä toimet on suoritettava muulloin kuin vaalien aikana.*

Järjestelmän kriittisin tekninen toimi on sen toteutus eli suunnittelu ja ohjelmointi.

Mikäli toteutuksessa on yksikin kriittinen osa-alue, johon pieni joukko ihmisiä (esimerkiksi hypoteettisia lahjottuja tai hutiloivia ohjelmoijia) pääsee vaikuttamaan ilman valvontaa, on olemassa väärinkäytöksen tai tahattoman ohjelmointivirheen riski.

Euroopan neuvoston vaatimus kahden henkilön työryhmästä ja niiden kokoonpanon muuttamisesta on minimivaatimus, mutta tämä tulee ulottaa myös ohjelman kirjoitukseen ja tästä tulisi olla selkeä näyttö.

Meillä ei ole tietoa siitä, noudatettiinko näitä vaatimuksia järjestelmän kehityksen aikana.

> *57. Laskennasta on pidettävä pöytäkirjaa, johon merkitään tiedot laskennan alkamisesta ja lopettamisesta sekä siihen osallistuneista henkilöistä.*

Kuten aiemmin tässä dokumentissa esitettiin (suositusten 23 ja 56 osalta), sähköisessä äänestyksessä itse laskentaa ei suorita laskentatyöaseman käyttöhenkilöstö vaan itse asiassa laskentatyöasemassa suoritettava tietokoneohjelma.

Sähköisiä tuloksia eivät siis laskeneet Helsingin vaalipiirilautakunta ja Oikeusministeriö suoraan vaan he pelkästään käynnistivät ohjelman, joka laskennan suoritti.

Laskennan suorittava ohjelma puolestaan tekee niitä asioita, joita sen ohjelmoija on sen käskenyt tehdä. Sen vuoksi, mikäli halutaan tunnistaa kaikki laskennan kanssa

tekemisissä olevat henkilöt, ovat he ohjelman kirjoittajia (joita on todennäköisesti useampia). Nämä mahdollisesti ulkomaiset henkilöt osallistuvat siis suomalaiseen vaalitulosten laskentaan suoralla ja konkreettisella tavalla.

Effi huomauttaa lisäksi, että perinteiset paperiset äänestyslipukkeet laskevat kilpailevien puolueiden edustajat. Sen lisäksi, että kilpailijoiden voi olettaa valvovan toisiaan, ääntenlaskenta on hyvin hajautettu. Laajan huijauksen toteuttaminen vaatisi usean äänestyspaikan ääntenlaskennan huijausta. Ennakkoäänestyksen ennakkoäänet lasketaan keskusvaalilautakunnassa, jonka kokoonpano on niinikään eri puolueista.

59. Sähköisen äänestysjärjestelmän tulee olla tarkastettavissa.

Turun yliopiston auditointiryhmä auditoi sähköisen äänestysjärjestelmän. Oikeusministeriö on julkaissut aditointiraportin[18], ja sitä on kommentoitu Effin toimesta[19].

Uskomme myös, että järjestelmä on niin monimutkainen, että täydellinen auditointi olisi liian kallista. Tämä liittyy alla mainittuihin vaatimuksiin 75 ja 92.

> *75. Tärkeiden sähköisten vaalien tai kansanäänestysten toimittamisessa tarvittavien laitteiden on sijaittava turvallisessa paikassa ja tätä paikkaa on koko vaalin tai kansanäänestyksen ajan suojattava kaikenlaiselta ja kenen tahansa aiheuttamalta häiriöltä. Vaalien tai kansanäänestyksen ajaksi on laadittava toipumissuunnitelma. Lisäksi kaikki tieto, joka säilytetään vaalien tai kansanäänestyksen jälkeen, on varastoitava turvallisesti.*

Laitteiden turvallinen varastointi on riski, joka on esimerkiksi Yhdysvalloissa osoittautunut suureksi. Äänestyskoneita on löydetty vartioimattomana äänestyspaikoilta[20]. Tämän vuoksi tähän riskiin on suhtauduttava vakavasti.

On kuitenkin kyseenalaista, pystyykö muu kuin tietotekniikan alan ammattilainen näkemään, onko laitteessa esimerkiksi mitään ylimääräistä. Sähköisessä äänestyksessä käytettiin tavanomaista PC-laitteistoa. Tällaisessa laitteistossa on yleensä huomattava määrä erilaisia liitäntöjä, esimerkiksi USB-liitäntöjä, joista kaikki eivät välttämättä ole näkyvissä koneen ulkopuolella. Vaikka koneet käynnistettäisiin erityiseltä käynnistyslevyltä, kone voi silti ensin ajaa ohjelmia, jotka on ujutettu sisään tällaista

---

[18] Auditointiraportti kunnallisvaalien sähköisen äänestyksen pilotista. Turun yliopisto, 13.6.2008. http://www.vaalit.fi/uploads/6d8qgeom5g.pdf

[19] Effin blogi 4.9.2008. http://www.effi.org/blog/kai-2008-09-04.html

[20] Ed Felten on yhdysvaltalainen tietoturva-alan ammattilainen, joka on sattunut tällaiseen tilanteeseen jo kahdesti: http://www.freedom-to-tinker.com/?p=1253 sekä http://www.freedom-to-tinker.com/?p=1084.

liityntää käyttäen. Tämäkään riski ei ole tuulesta temmattu, vaan sekin on jo havaittu Yhdysvalloissa[21].

Laitteistoon tehdyt muutokset voivat olla paljaalla silmällä havaitsemattomissa, sillä ne voivat sijaita esimerkiksi komponenttien sisäisessä ohjelmistossa, nk. firmwaressa. Muutokset on saatettu tehdä jo ennen, kuin koneet on toimitettu äänestysviranomaisille. Effi haluaisikin kiinnittää huomiota myös koko siihen ketjuun, jota pitkin laitteisto toimitetaan, ei pelkästään siihen, mitä laitteille tapahtuu sen jälkeen, kun äänestysviranomaiset ovat saaneet ne haltuunsa.

> *92. Riittävin toimenpitein on varmistettava, että äänestäjän äänestykseen käyttämä järjestelmä voidaan suojata sellaisilta vaikutuksilta, jotka voisivat muuttaa ääntä.*

Äänestykseen käytettävä järjestelmä itsessään vastaa äänen oikeellisuudesta ja niinpä kaikkein kriittisin osa, joka saattaisi muuttaa ääntä, on äänestyskoneen ohjelmisto.

Kuten tässäkin dokumentissa on jo useasti aiemmin todettu, ohjelmiston toimintaa ei loppukäyttäjä voi käytännössä ulkoisesti seurata. Se, että ohjelmisto näyttää ruudulla oikean ehdokkaan numeron ja äänestäjä hyväksyy sen, ei itsessään takaa äänen rekisteröitymistä oikealle ehdokkaalle, vaan se edellyttää kaikkien tähän osallistuvien ohjelmistokomponenttien olevan luotettavia. Tämä ongelma nostettiin myös esille auditointiraportissa.

Tätä ongelmaa oltaisiin voitu rajata muun muassa käyttämällä järjestelmän laskentaytimen toimittajan tarjoamaa sähköistä kuittia, joka jää äänestäjälle: *"Pnyx generates a voting receipt that allows each individual voter to verify the correct treatment of his/her vote"*. Kuitista itsestään ei pysty päättelemään, mitä äänestäjä äänesti, koska se voisi johtaa kiristykseen ja äänten ostoon[22]. Kuitin avulla kuitenkin äänestäjä olisi voinut varmistua siitä, että hänen äänensä on mennyt perille. Suomen järjestelmässä tätä vaihtoehtoa ei kuitenkaan käytetty.

Ongelman ei tarvitse aina olla edes ohjelmistossa. Yhdysvalloissa käytetyissä äänestyskoneissa on havaittu ongelmia kosketusnäytön kalibroinnissa[23]. Tämä aiheuttaa sen, että käyttäjän koskettaessa jotakin kohtaa ruudulla ohjelmisto tulkitsee kohdan olleen jonkin toisen.

---

[21] Ks. "Boot loader reflashing", dokumentissa Diebold TSx Evaluation. Harri Hursti, 11.5.2006. http://www.blackboxvoting.org/BBVtsxstudy.pdf

[22] On myös olemassa äänestysprotokollia, joissa kuitin avulla voidaan myös tarkistaa, että ääni on laskettu oikein. Sen perusteella, mitä Scytlin materiaalista olemme ymmärtäneet, tätä mahdollisuutta vaaleissa käytössä olleen Pnyxin version kuitti ei kuitenkaan näyttäisi mahdollistavan.

[23] Jälleen Ed Feltenin blogi, http://www.freedom-to-tinker.com/index.php?p=707.

Suomen järjestelmässä tämä ei ollut niin suuri ongelma, koska äänestäjän on vielä varmistettava numeron oikeellisuus. Kuitenkin tämä on hyvä esimerkki siitä, että ongelma voi olla lähes missä tahansa laitteen osassa, joka jollakin tavalla liittyy äänen käsittelyyn. Näitä osia – sekä laitteiston että ohjelmiston osia – on huomattava määrä[24], ne tulevat eri puolilta maailmaa ja kaikkien niiden sisällön tutkiminen olisi erittäin kallista.

> *107. Tarkastusjärjestelmän on kyettävä tarkistamaan ja varmistamaan, että sähköinen äänestysjärjestelmä toimii asianmukaisesti ja että tulos on oikein sekä havaitsemaan äänestäjän tekemät petokset ja todistamaan että kaikki lasketut äänet ovat oikeita ja että kaikki äänet on laskettu.*

Effin kanta on, että sähköisessä äänestyksessä pitäisi käyttää äänestäjän varmentamaa paperitulostetta. Tällöin äänestäjä äänestäisi koneella, mutta sähköisen uurnan lisäksi kone tulostaisi perinteisen äänestyslipun, jonka äänestäjä tarkistaisi ja joka pudotettaisiin perinteiseen uurnaan. Näiden paperitulosteiden tarkistaminen olisi riittävän erillinen tapa varmistua järjestelmän oikeasta toiminnasta.

On tietenkin niin, että paperituloste mitätöisi joitakin sähköäänestyksen eduista, mutta tarkisteita ei ehkä tarvitsisi laskea kuin pistokokeina tilastollisesti riittävä määrä sekä väärinkäytösepäilyjen sattuessa ehdokkaiden vaatimuksesta.

Yhdysvalloissa tämän kaltainen paperituloste, englanniksi VVPT, VVPR tai VVPB (Voter Verified Paper Trail / Record / Ballot), on jo vaatimuksena 32 osavaltiossa[25]. Myös Alankomaissa paperitulosteen käyttöönottoa on esitetty[26], joskin siellä vaatimus nähtiin niin hankalana, että sähköisestä äänestämisestä luovuttiin mieluummin toistaiseksi kokonaan[27].

Effin mielestä ei ole mitään syytä, miksi Suomessa käyttöön otettava järjestelmä olisi jotenkin oleellisesti luotettavampi kuin yhdysvaltalainen tai alankomaalainen. Tästä syystä äänestäjän varmentama paperituloste on vaadittava myös meillä.

---

[24] Käytettävyyden ja tietoturvan asiantuntija Ka-Ping Yee on piirtänyt kuvan tyypillisen sähköäänestysjärjestelmän osista. Mikä tahansa osa saattaisi vaikuttaa annettuun ääneen. http://usablesecurity.com/2006/02/23/the-election-software-supply-chain/

[25] http://www.verifiedvoting.org/

[26] Stemmen met vertrouwen. Adviescommissie inrichten verkiezingsproces. 27.9.2007. http://www.minbzk.nl/108589/stemmen-met

[27] Alankomaiden sisäministeriön kirje alahuoneen puhemiehelle 16.5.2008. http://www.wijvertrouwenstemcomputersniet.nl/images/7/7b/Briefaantweedekamerovenrichtingverkiezingsproces.pdf

Lisätietoja

Effi on kerännyt verkkosivulleen listan usein kysytyistä kysymyksistä sähköisen äänestämisen suhteen. Vastauksissamme selvitämme muun muassa, miksi sähköisen äänestämisen vertaaminen nettipankkiin ei toimi. Effin sähköäänestys-FAQ on luettavissa osoitteessa http://www.effi.org/sahkoaanestys-faq.html.

Uusin versio tästä dokumentista on saatavilla Effin verkkosivuilta, http://www.effi.org/.

Tämän dokumentin tekijänoikeuksista on luovuttu (public domain).

Liite 1

Oikeusministeriön perustelu sille, että he eivät luovuta äänestysjärjestelmään liittyviä asiakirjoja[28]:

> *Viranomaisten toiminnan julkisuudesta säädetyn lain (621/1999, JulkL) 24.1 §; n 7 kohdan mukaan tietojärjestelmän turvajärjestelyjä ja niiden toteuttamista kuvaavat asiakirjat ovat salassa pidettäviä, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna turvajärjestelyjen tarkoituksen toteutumista. Yksityiskohtaiset tekniset kuvaukset ovat säännönmukaisesti salaisia, eikä sellaisia siksi voida antaa luettavaksi (ks. hallituksen esitys eduskunnalle laiksi viranomaisten toiminnan julkisuudesta ja siihen liittyviksi laeiksi, HE 30 1998 vp, s. 91).*

Effin kommentti: fyysiset turvajärjestelyt, kuten äänestyskoneiden säilytys, ovat luontevasti salassa pidettävää tietoa. Samaten on ymmärrettävää, että vaikkapa pankit eivät kerro tietojärjestelmistään niille, joille tieto ei kuulu. Kuitenkin, sikäli kun kyse on ohjelmistoista, joita käytetään demokraattisissa vaaleissa, ohjelmistojen tulisi olla turvallisia, vaikka niiden kaikki turvamekanismit ja koko sen lähdekoodi (ohjelmisto) olisivat julkisia. Tämä tunnetaan nk. Kerckhoffsin periaatteena[29] ja se on yleisesti hyväksytty tietoturvan suunnittelussa.

> *JulkL:n 24.1 §:n 20 kohdan mukaan salassa pidettäviä viranomaisen asiakirjoja ovat myös asiakirjat, jotka sisältävät tietoja yksityisestä liike- tai ammattisalaisuudesta, samoin kuin sellaiset asiakirjat, jotka sisältävät tietoja muusta vastaavasta yksityisen elinkeinotoimintaa koskevasta seikasta, jos tiedon antaminen niistä aiheuttaisi elinkeinonharjoittajalle taloudellista vahinkoa, ja kysymys ei ole kuluttajien terveyden tai ympäristön terveellisyyden suojaamiseksi tai toiminnasta haittaa kärsivien oikeuksien valvomiseksi merkityksellisistä tiedoista tai elinkeinonharjoittajan velvollisuuksia ja niiden hoitamista koskevista tiedoista.*

Effin kommentti: kun kyse on demokraattisista vaaleista, niiden toteutus ei missään tapauksessa saa olla minkään yrityksen liikesalaisuus. On muistettava, että äänten laskennan suorittaa ohjelmisto eikä ohjelman käyttäjä. Effin näkemyksen mukaan laskennan pitäminen liikesalaisuutena haittaa äänestäjien ja ehdokkaiden oikeuksien valvontaa.

---

[28] Oikeusministeriön sähköinen vastaus dokumenttipyyntöön 29.2.2008.

[29] http://en.wikipedia.org/wiki/Kerckhoffs%27_principle