Julkisuus äänestysverkon turvallisuuden takaajana

ARTO TENGVALL

Hannu Nurmi ja Arto Salomaa esittelivät *Politiikka* 1/91:ssä kehittämänsä menetelmän, jossa äänestäminen suoritettaisiin kryptografisen protokollan avulla tietokoneitse. Menetelmä mahdollistaa etääänestämisen niin, että äänestyssalaisuus säilyy ja äänestäjällä on myös mahdollisuus peruuttaa antamansa ääni.

Esitelty menetelmä on monessa suhteessa varsin ansiokas. Kryptografisen äänestysprotokollan heikkous on kuitenkin sen monimutkaisuus, jonka vuoksi enemmistö kansalaisista, näin pelkään, ei osaa eikä halua käyttää sellaista valtiollisissa äänestyksissä ja vaaleissa. Siksi esitin *Politiikka* 3—4/91:ssä oman, äänestäjäystävällisen versioni tietokoneistetusta äänestysmenettelystä.

Äänestyksen teknisten järjestelyjen lisäksi kiinnitin huomiota myös huomattavasti oleellisempaan asiaan: aiheen poliittiseen sisältöön. Vaalien tietokoneistaminen ei ole tavoite sinänsä. Kysymys on pikemminkin siitä, miten tietokoneistettua äänestysmenettelyä voidaan käyttää demokratian edistämiseksi. Ehdottamani äänestysverkko mahdollistaisi sen, että nykyinen *jaksoittainen äänioikeus* (jota käytettäessä äänestäjäkunta ja sen vaikutusvalta joutuvat vaalien jälkeen aina neljäksi vuodeksi pakkolomalle) voitaisiin laajentaa *jatkuvaksi äänioikeudeksi.* Jatkuva äänioikeus tarjoaisi nykyistä edistyneempiä menetelmiä sekä suoran että välillisen demokratian harjoittamiseksi. Tällöin yksittäinen kansalainen voisi valita asiakohtaisesti sen, osallistuuko päätöksentekoon henkilökohtaisesti vai asettamansa valtuutetun välityksellä.

Nurmi ja Salomaa vastasivat kirjoitukseeni *Politiikka* 2/92:ssa. He epäilivät, että en ollut kylliksi huomioinut kaikkia turvallisuusnäkökohtia, joita hahmottelemani äänestysverkko edellyttää. Koska tämä puoli asiasta jäi kirjoituksessani kieltämättä turhan ylimalkaiseksi, haluan vastata Nurmen ja Salomaan esittämiin kysymyksiin.

Äänestysverkon turvallisuustekijät

Nurmi ja Salomaa kirjoittavat: »Meillä on Tengvallia oleellisesti epäluuloisempi asenne niihin henkilöihin, jotka huolehtivat äänestysjärjestelmän rakentamisesta, käyttöönotosta ja toiminnasta.» He korostavat aivan oikein, että vaaleissa ja äänestyksissä käytettävän järjestelmän tulee kyetä eliminoimaan myös teknisen henkilökunnan mahdollisuudet vilpintekoon.

Persoonallisuuteeni kuuluva yleinen patologinen epäluuloisuus pätee kyllä myös tässä asiassa. Vaikka talletankin varojani pankkitilille ja suoritan maksujani pankkisiirtona — kuten oletettavasti tekevät myös Nurmi ja Salomaa — olen taipuvainen vaatimaan äänestysverkolta kaikin osin suurempaa turvallisuutta kuin niiltä pankkien tietokonejärjestelmiltä, jotka nykyisin huolehtivat meidän kaikkien rahoistamme.

Mihin perustuu se, että yhteisestä epäluottamuksestamme huolimatta olemme valmiit uskomaan varamme pankkien tietokonejärjestelmien hoidettavaksi? »Varomattomuutemme» syynä on uskomus, jonka mukaan niissä suoritettava vilppi olisi riittävän suurella todennäköisyydellä paljastettavissa. Kysymys ei toki ole absoluuttisesta turvallisuudesta. Se olisi saavutettu vasta, jos mikään vilppi ei olisi edes teoriassa mahdollinen — eli mikäli vilpin tekemiseen tarvittavat toimenpiteet olisivat loogisesti mahdottomia suorittaa.

Yksikään koskaan käytetty tai ehdotettu äänestysjärjestelmä tai pankkien varainsiirtojärjestelmä,

tietokoneistettu tai manuaalinen, ei ole kokonaisuutena absoluuttisen turvallinen. Tällaisissa monimutkaisissa systeemeissä absoluuttinen turvallisuus voidaan taata vain määrättyjä vilpinteon muotoja vastaan. Muita väärinkäytöksiä vastaan on suojauduttava siten, että vilpinteon onnistuminen tehdään mahdollisimman epätodennäköiseksi ja pelkän yrityksenkin välitön ilmitulo mahdollisimman todennäköiseksi, ja siten, että sanktioidaan tällaiset yritykset ankarilla rangaistuksilla.

Mikä sitten on riittävä turvallisuustaso? Se turvallisuusajattelu, johon perustuen olen suunnitellut *Politiikka* 3—4/91:ssä esittelemäni äänestysverkon, täyttää seuraavat turvallisuuskriteerit:

1a. Äänten laskennan manipulointi, äänestyssalaisuuden murtaminen, sekä äänten väärentäminen ovat loogisesti mahdottomia niin ulkopuolisten tahojen kuin äänestysverkon ylläpitohenkilöstön yksittäisten jäsentenkin suoritettaviksi.

1b. Se, että tarvittava määrä avainhenkilöitä liittoutuisi väärinkäytöksiä varten, on tehty inhimillisesti katsoen mahdottomaksi.

1c. Mikäli tällainen salaliitto silti syntyisi, sen on loogisesti mahdotonta suorittaa edellämainittuja tekoja paljastumatta välittömästi vähintään useille tuhansille kansalaisille.

Verkon rakenne tekee loogisesti mahdottomaksi ohjelmoinnin muualta kuin keskusyksikön välittömässä läheisyydessä sijaitsevasta eristetystä toimipisteestä, ohjelmointiasemasta käsin. Aseman lukituksen ohittaminen vaatii useamman eri henkilöille hajautetun erilaisen magneettikortin. Samoin ohjelmoinnin aloittaminen, mikä oikeiden korttien lisäksi vaatii myös oikeiden salasanojen käyttöä. Korttien hallussapitäjät valitaan arpomalla laajasta eri tahojen nimittämien kandidaattien joukosta ja vaihdetaan säännöllisesti.

Ohjelmointiaseman väkivaltainen haltuunotto ei näin ollen yksin riitä väärinkäytösten suorittamiseen. Rauhanomaisemman petoksen edellyttämää salaliittoa ei voi muodostua, koska siihen täytyisi onnistua värväämään liian monta liian usein vaihtuvaa henkilöä. Ohjelmiston manipulointi edellyttäisi siis useiden henkilöiden sieppauksia, heidän pakottamistaan yhteistyöhön ja ohjelmointiaseman haltuunottoa. Tätä kaikkea on mahdotonta suorittaa salassa.

2. Pienten, kenen tahansa tehtävissä olevien väärinkäytösten onnistuminen on epätodennäköistä ja vahingot helposti korjattavissa.

Esim. jos varastaa toiselta äänestyskortin, tulee myös kyetä selvittämään vaadittava salasana. Kortin oikea omistaja voi marssia poliisilaitokselle, mitätöidä kadonneen korttinsa ja saada tilalle uuden. Vaikka varas olisi saanut salasanankin selville, voi äänioikeutettu uuden korttinsa avulla mitätöidä ne suoritukset, joita varas on tehnyt hänen nimissään (paitsi mikäli kyseisen asian äänestysaika on ehtinyt tällä välin umpeutua). Äänestyskortin huomaamaton lainaaminen sen kopioimiseksi johtaa samaan tulokseen. Äänestyspääte tekee korttiin kunkin äänestyskerran jälkeen merkinnän, joten täydellisesti kopioitu korttikin paljastuu heti kun äänioikeutettu yrittää käyttää alkuperäistä korttia.

3. Verkon tarvitsemien tietojen ylläpidosta huolehtivat viranomaiset eivät voi huomaamattomasti luoda ylimääräisiä äänioikeutettuja eivätkä mitätöidä todellisia. Verkkoon syötettyä äänioikeutettujen luetteloa koskevia muutoksia tekevät ainoastaan muutamat valtuutetut henkikirjoitusviranomaiset. Tämä voidaan tehdä vain muutamista keskustietokoneen tunnistamista päätteistä käsin kyseisen henkikirjoittajan omalla salaisella puumerkillä vahvistettuna. Lisäksi jokainen tällainen toimenpide on julkinen tulostuen automaattisesti sadoissa erillisissä toimipisteissä. Siten väärinkäytökset, niiden tekopaikka sekä tekijä paljastuvat välittömästi.

Aivan sama koskee niitä toimenpiteitä, joilla äänestysviranomainen syöttää verkkoon vaalien ehdokasasettelua ja kansanäänestysten kysymyksenasettelua koskevan informaation.

4. Äänestystietojen muuttaminen on loogisesti mahdotonta (ohjelmallisten keinojen lisäksi) muutoin kuin tarkoitukseen varatuilta äänestysautomaateilta, äänestyskortin ja sitä vastaavan tunnusluvun avulla. Myöskään äänestysviranomaisten tai henkikirjoittajan syöttämien tietojen muuttaminen verkon ulkopuolelta käsin ei ole loogisesti mahdollista.

Verkon keskustietokoneeseen tai sen päätteisiin saa yhteyden vain verkkoon vartavasten kytketyistä päätteistä. Kryptologisin keinoin tehdään loogisesti mahdottomaksi myös se, että joku kytkeytyisi puhelinlinjalla tällaisen päätteen ja keskustietokoneen väliin ja pääsisi siten yhteyteen keskustietokoneen tai päätteen kanssa.

Tässä kohdassa on kryptologialla siis tärkeä osuus äänestysverkon toiminnassa. Laitteisto sa-

lakirjoittaa kunkin verkkoon kytketyn päätteen ja verkon keskustietokoneen välisen kommunikaation automaattisesti siten, että (a) keskustietokone tunnistaa sen päätteen, johon on yhteydessä, ja pääte tunnistaa keskustietokoneen (muualta tulevaa dataa ei vastaanoteta), ja siten, että (b) kenenkään on mahdotonta jäljitellä äänestyspäätettä, henkikirjoittajan päätettä tai äänestysvirkailijan päätettä ja syöttää minkäänlaista dataa keskustietokoneelle tai välittää keskustietokoneena esiintyen dataa näille päätteille tai järjestelmän tulostusyksiköille, sekä siten, että (c) keskustietokoneen ja päätteen välistä kommunikointia on mahdotonta tulkita puhelinlinjaa salakuuntelemalla.

5. Verkon ohjelmiston virheettömyyden varmistus. Mikäli oikein ymmärsin, Nurmen ja Salomaan huoli kohdistui ensisijaisesti juuri tähän asiaan. Käsittelenkin aiheen seuraavaksi seikkaperäisesti omana kokonaisuutenaan.

Ohjelmointi ja siihen sisältyvien riskien hallinta

Mitään tietokoneohjelmistoa ei voi valmistuttaa siten, etteikö valmistaja voisi yrittää kätkeä siihen salattuja ominaisuuksia. Ongelma onkin näin ollen siinä, että tällaisten yritysten paljastuminen on tehtävä kerta kaikkiaan väistämättömäksi. Kun järjestelmän koko ohjelmisto on kerran saatu virheettömänä asennetuksi, ei sen looginen rakenne enää anna mahdollisuuksia ohjelmiston salaiseen muuttamiseen.

Jos samat henkilöt saisivat laatia millaisen tahansa äänestysjärjestelmän (itseni, Nurmen ja Salomaan tai kenen tahansa muunkaan ideoiman) tai minkä tahansa muun arkaluontoista tietoa käsittelevän systeemin tietokoneohjelmat, testata ne, asentaa ne käytettävään järjestelmään ja toimia vielä järjestelmän ylläpitäjinäkin, olisi tilanne luonnollisesti absurdi. Mistä äänestäjä voisi tietää, että tietokonejärjestelmä toimii juuri sillä tavalla kuin hänelle sanotaan sen toimivan?

Äänestäjän ei tule joutua sokeasti luottamaan äänestysverkon ohjelmoivien asiantuntijoiden vilpittömyyteen. Keinot, joita ehdotan ohjelmiston luomisen ja asennuksen valvomiseksi, ovat moninkertaisesti varmempia kuin yksikään aiemmin käytetty tai ehdotettu menetelmä minkään tietojärjestelmän ohjelmoijien kontrolloimiseksi. Joko tällaisia tai näistä supistettuja menetelmiä olisi käytettävä jokaisen arkaluontoisen ohjelmistopaketin yhteydessä. Myös Nurmen ja Salomaan malli edellyttäisi jotakin vastaavaa.

Olen lähtenyt siitä, että yksikään ohjelmiston tekemiseen osallistuva henkilö ei saa kyetä muiden mukanaolijoiden huomaamatta ujuttamaan salaisia käskyjä eli »takaportteja» ohjelmistoon, ja siitä, etteivät kaikki nämä henkilöt yhdessäkään voisi tätä tehdä ilman täysin varmaa kiinnijäämistä.

Ohjelmiston luominen alkaa systeemisuunnittelusta. Tehtävään palkatut asiantuntijat valitsevat tarvittavan laitteiston ja suunnittelevat, minkä kaltaisia ohjelmia äänestysjärjestelmään tarvitaan ja miten näiden ohjelmien tulee kontrolloida sekä toinen toisiaan että järjestelmän käyttäjiä.

Sen jälkeen pyydetään alan asiantuntijoita ilmoittautumaan tarvittavan sovellusohjelmiston tekijöiksi. Kutakin ohjelmiston osaa tekemään tulee työryhmä, joka arvotaan tehtävään tarjoutuneiden asiantuntijoiden joukosta. Kaikki ohjelmia ei tarvitse luoda alusta alkaen, koska suuri osa räätälöidään joistakin jo käytössä olevista ohjelmista. Kun työ on valmis, julkistetaan aikaansaatu ohjelmalistaus sekä kuvaus ohjelman toiminnasta. Kuka tahansa kylliksi tietokoneiden ohjelmoinnista ymmärtävä voi siis tutustua ohjelmalistaukseen ja julkistaa mielipiteensä sen toiminnasta — mukaan lukien ohjelman sisältämät virheet ja turvallisuusongelmat.

Tähän liittyen tehdään tarjous: jokainen, joka osoittaa jossakin listatun ohjelmiston osassa tai niiden muodostamassa kokonaisuudessa manipulaation mahdollistavan takaportin, saa palkkioksi 10 miljoonaa markkaa — ja ohjelman kehittänyt työryhmä menettää palkkionsa. Joku joutunee asiasta myös syytteeseen. Vähemmän vaarallisten virheiden löytäjä saa 100.000—1.000.000 markkaa.

Kaikki tarkistukset tehdään ohjelman listauksesta, ei tallennetusta ohjelmasta. Jälkimmäiseen on mahdollista piilottaa salaisia takaportteja, edellisestä asiantuntija ei voi olla niitä löytämättä. Esimerkiksi sanomalehdessä paperikopiona julkaistu ohjelmalistaus siis luetaan skannerilla eli optisella lukijalla tietokoneen muistiin ja tallennetaan alkuperäisen kanssa identtisenä ohjelmana.

Samanaikaisesti kaksi arvotuista asiantuntijoista (joista yksikään ei ollut mukana ohjelmia kehitelleissä työryhmissä) koostuvaa työryhmää testaa koko ohjelmistopaketin autenttisella laitteistolla. Kumpikin raportoi havaintonsa itsenäisesti.

Kun ohjelmisto on saatu tarkastetuksi, on se saatava taatusti alkuperäisenä asennetuksi äänestysverkon keskustietokoneeseen. Keskustietokoneessa ei valmiiksi ole yhtäkään ohjelmapätkää,

ei edes käyttöjärjestelmää. Se on tässä vaiheessa ohjelmallisesti täysin neitseellisessä tilassa.

Mikä varmistaa sen, että ohjelmisto on juuri se julkistettu ja testattu ohjelmisto ilman mitään muutoksia, poistoja tai lisäyksiä? Vastaus löytyy vertailuohjelmista (vastaavista kuin mikrotietokoneiden DOS-käyttöjärjestelmään sisältyvät Comp ja FC). Sellaisen avulla voi tarkistaa bitti bitiltä kaksi ohjelmaa, ja vertailuohjelma ilmoittaa heti, jos ne eroavat toisistaan yhdenkin bitin verran.

Keskustietokoneeseen asennettavan ohjelmiston kunkin osan ovat useat eri ihmiset lukeneet skannerilla — julkistetusta paperilistauksesta — ja tallentaneet disketille tai nauhalle. Näiden ohjelmien tulisi siis olla keskenään identtiset. Mikäli tässä ei ilmene yllätyksiä, voidaan ne kopioida keskustietokoneeseen.

Nuo ihmiset on valittu arpomalla tehtävään tarjoutuneiden kansalaisten joukosta. Lisäksi mukana on yksi edustaja kustakin puolueesta.

Ohjelmien vertailua ja asennusta saamme ihailla suorassa TV-lähetyksessä. Näemme puolueiden asettamien edustajien ja kansalaistarkkailijoiden kunkin vuorollaan tarkistavan sen, että keskusyksikköön asennetaan juuri heidän asianmukaisesti skannerilta lukemansa ohjelma — tai vertailussa sen kanssa identtiseksi osoittautunut ohjelma.

Mitä tämä menettely merkitsee ohjelmistoturvallisuuden kannalta? Väärinkäytöksiä suunnittelevien tulisi muodostaa salaliitto, jossa olisivat mukana vähintään kaikki tietyn ohjelman tekemiseen osallistuvat henkilöt ja lisäksi jokainen virallisen testausryhmien jäsen. Tämä on kohtuullisen vaativa tehtävä ottaen huomioon, että nämä henkilöt eivät etukäteen, ennen tehtäviensä aloittamista, ole kenenkään tiedossa. Kuka tahansa voi palkatun henkilöstön ulkopuoleltakin voi osallistua testaukseen — sikäli kuin shokkilöydöksistä luvattu 10 miljoonaa markkaa jotakuta sattuisi kiinnostamaan.

En luota erityisen paljoa ohjelmointieksperttien rehellisyyteen, mutta tämän haasteen kohdalla luotan sitäkin vankemmin ulkopuolelle suljettujen ahneuteen ja mukana olevien kykenemättömyyteen peittää jälkensä edellisiltä.

Keskustietokoneen ohjelmiston varsinainen asennus on, kuten saatoimme havaita, varsin nopea ja yksinkertainen toimenpide. Kysymys on tunneista, ei vuorokausista. Kun ohjelmiston asennus on suoritettu loppuun, ei ohjelmointiasemaan ole enää pääsyä. Järjestelmää hoitava vakituinen henkilöstö ei siis ohjelmoi mitään, vaan joutuu toimimaan kokonaan alunperin asennettujen ohjelmien varassa. Niiden joukossa olevat tarkistusohjelmat hälyttävät jokaisesta toimenpiteestä — tahattomasta tai tahallisesta — joka voisi uhata äänestyssalaisuutta tai äänten asianmukaista laskentaa.

Mikäli ohjelmistoa ajan myötä tarvitsee uusia, menetellään edellä kuvattua vastaavalla tavalla.

Sabotaasi ja käyttöhäiriöt

Paitsi keskustietokoneen omista ohjelmista ja niiden käyttäjistä, olivat Nurmi ja Salomaa huolissaan myös esittämäni järjestelmän reagoinnista mahdollisiin toimintahäiriöihin tai sabotaasiin.

Kun puhumme tämän kokoluokan tietokonejärjestelmistä, voimme kokonaan sivuuttaa sähkökatkot yms. Varageneraattorin ansiosta tällaiset ulkopuoliset häiriöt eivät voi vaikuttaa keskustietokoneen toimintaan. Koneen sammuminenkaan ei olisi ongelma, sillä kaikki tiedostot on talletettu pysyvään massamuistiin, joten ohjelmisto voidaan välittömästi ladata uudelleen käynnistämällä kone.

Pelko tietokoneviruksista tms. ulkoapäin suoritettavasta ohjelmistollisesta sabotaasista on ammattimaisen tietokoneenkäyttäjän arkipäivää. Se koskee jokaikistä tietokoneverkkoa, ei ainoastaan minun esittämääni äänestysverkkoa. Siksi suuremmissa järjestelmissä on usein käytössä portinsuojauslaite, joka tarkistaa jokaisen keskustietokoneelle ulkoa päin — eli siis puhelinlinjoja pitkin — tulevan yhteydenoton. Äänestysverkkoon ei päästetä muita viestejä kuin ne, jotka (a) on lähettänyt jokin järjestelmän tunnistama siihen kuuluva laite ja jotka (b) on »allekirjoittanut» järjestelmän tunnistama henkilö ja jotka (c) pitävät sisällään ainoastaan senlaatuista dataa, jota viestin kohteena oleva pääte tai keskustietokone on ohjelmoitu käyttämään.

Sabotöörin tulee siis käyttää räjähteitä tms. välineitä, joiden kanssa ei järjestelmän arimpiin kohtiin niin vain marssita. Jos keskustietokone todella tulee tuhotuksi, on jatkuva äänioikeus epäilemättä pantava vähäksi aikaa jäihin. Eduskunnan voimasuhteet pysyvät viimeisen äänestyspäivän tilannetta vastaavina ne viikot, jotka tarvitaan uuden järjestelmän asentamiseen.

Joitakin lisähuomautuksia

Nurmi ja Salomaa esittivät joitakin epäilyksiä siitä, antaisiko esittämäni malli mahdollisuuden joihinkin kenelle tahansa mahdollisiin väärinkäytöksiin.

Esitin, että äänestäjä, joka olisi hukannut sekä salasanansa että äänestyskorttinsa, voisi tilata viranomaisilta äänestystietonsa sisältävän hakemiston tuhoamisen ja saada tällöin vastineeksi uuden lokeron ja sen vastineeksi uuden äänestyskortin. Tämä kirvoitti kysymyksen, voisiko joku tuhota samalla tavalla muidenkin äänestäjien lokeroita.

Vastaus: ei voi. Hakemiston tuhoaminen ei sentään onnistuisi pelkällä puhelinsoitolla — siis antamalla henkilön nimi ja pyytämällä uuden äänestyskortin lähettämistä johonkin postilokeroon (Pankeistakaan ei näin helposti saa toisten ihmisten tileihin liittyviä pankkikortteja.) Hakemiston tuhoaminen tilattaisiin tekemällä siitä vaatimus henkilökohtaisesti poliisilaitoksella, henkilöllisyystodistuksen kanssa ja kahden todistajan varmentaessa asiaa koskevan lomakkeen. Jos joku onnistuisi väärennetyin paperein tekemään tämän tempauksen, ei tilanne silti olisi korjaamaton. Kun lokeron oikea omistaja seuraavana päivänä saa postissa ilmoituksen lokeronsa tuhoamisesta (tai havaitsee tämän itse äänestyspäätteeltä), saamme hyvin pian tutustua poliisiasemalla myös häneen.

Epäilyjä herätti erityisesti kielikuva »lokeron avaaminen». Ilmaisu ei ilmeisesti ollut erityisen onnistunut kuvaamaan tilannetta, jossa salasanansa unohtanut äänestäjä pyytää salasanan poistamista »äänestyslokerostaan» eli voimassa olevat äänensä sisältävästä hakemistosta. Kysehän ei tietenkään ole siitä, mitä ajatus fyysisen lokeron avaamisesta ilmeisesti saattoi tuoda mieleen, vaan, kuten olin kirjoittanutkin, ainoastaan siitä, että kun salasana on poistettu hakemistosta, äänestäjä saa siihen yhteyden pelkällä äänestyskortillaan. (Ilman kyseisen äänestäjän äänestyskorttia kukaan ei nytkään saa yhteyttä hänen lokeroonsa.) Samalla hän voi ottaa itselleen uuden salasanan. Myöskin tämä salasanan poistaminen edellyttää henkilökohtaista käyntiä viranomaisten luona.

Koska mitään fyysistä lokeroa ei ole olemassakaan, vaan kyseessä on pelkkä magneettinauhalle salakirjoitettu tiedosto, ei kukaan voi todellakaan — käyttämästäni kielikuvasta »lokeron avaaminen» huolimatta — avata lokeroa ja katsoa, kuinka sen omistaja on äänestänyt. Se ohjelmointi, jolla tämän tyyppiset hakemistot on luotu ja jolla niitä käsitellään, ei hyväksy henkilökunnalta sellaista käskyä kuin »tulosta äänestäjälokeron sisältö». Tämän tiedon saaminen edellyttäisi siis koko systeemin ohjelmoinnin muuttamista. Mikä — kuten tästä kirjoituksesta aiemmin on tullut ilmi — on tehty mahdottomaksi.

Mainittu »äänestäjälokero» eli hakemisto ei myöskään sisällä äänestäjän koko äänestyshistoriaa, kuten Nurmi ja Salomaa olettivat. Se sisältää ainoastaan ne äänet, jotka äänestäjä on antanut sillä hetkellä käynnissä olevissa äänestyksissä tai vaaleissa. Kuten omassa kirjoituksessani olin — tosin eri kohdassa ja kieltämättä turhan epäselvästi — maininnut, »äänestysajan päätyttyä järjestelmä tulostaa äänestystuloksen ... ja tuhoaa äänestyslomakkeet» eli kunkin äänestäjän lokerossa olevan tiedon siitä, miten tämä henkilö on asiassa äänestänyt.

Lopuksi

Nurmen ja Salomaan vastine ansaitsee kiitoksen siitä tavasta, jolla he kiinnittivät huomiota kysymykseen äänestysverkon alkuperäisestä ohjelmoinnista ja sen sisältämistä turvallisuusongelmista. Toivottavasti olen kyennyt edellä antamaan tyydyttävän selonteon myös tästä asiasta.

Tietenkään tämä ei tule olemaan viimeinen sana aiheesta. On ilahduttavaa havaita, että tietokoneistetun äänestyksen ongelmiin kiinnitetään vakavaa huomiota ja että niille kehitellään kilpailevia ratkaisuja. Nurmen ja Salomaan laatima protokolla sisälsi eräitä ideoita, joita olen suoraan soveltanut oman mallini paranteluun. Kilpailu tunnetusti parantaa tuotteiden laatua.

Luultavasti tulemme jatkossa näkemään yhä yksinkertaisempia ja käyttäjäystävällisempiä malleja tietokoneäänestyksen järjestelyiksi; sellaisia malleja, jotka täyttäisivät sekä itse esittämäni että Nurmen ja Salomaan esittämät vaatimukset.

Ehkäpä aika alkaa olla kypsä sille, että myös jatkuvaan äänioikeuteen perustuvien poliittisten järjestelmien ideoinnissa voisi syntyä kilpailua. Tähän saakka aihepiiri tuntuu jääneen lähinnä Äänivalta ry:n monopoliksi — täysin vastoin yhdistyksen pyrkimyksiä.