



NETTIÄÄNESTYSTYÖRYHMÄN KOKOUS

Aika: 4.5.2017 klo 13.00-15.00

Paikka: Oikeusministeriö, Eteläesplanadi 10, kokoustila Kiinnitys

Osallistujat: ~~Puheenjohtaja:~~
~~Johtaja Johanna Suurpää, oikeusministeriö (estynyt)~~

Varapuheenjohtaja:
Vaalijohtaja Arto Jääskeläinen, oikeusministeriö

Jäsenet:
Markus Rahkola, valtiovarainministeriö
Mikko Viitaila, Viestintäviraston Kyberturvallisuuskeskus
Annina Tjurin, Oikeusrekisterikeskus
Juha Mäenalusta, Oikeusrekisterikeskus
~~Tommi Simula, Valtion tieto- ja viestintätekniikkakeskus Valtori~~
~~Pauli Pekkanen, Väestörekisterikeskus~~
Tuomas Aura, Aalto yliopisto
Seppo Virtanen, Turun yliopisto
Marianne Kinnula, Oulun yliopisto
Hanna Wass, Kansallinen vaalitutkimuskonsortio
Timo Karjalainen, Electronic Frontier Finland ry EFFI

Sihteerit:
Ylitarkastaja Heini Huotarinen, oikeusministeriö
Projektipäällikkö Anneli Salomaa, oikeusministeriö

Tommi Karttaavi, Kuntaliitto
Tarvi Martens, State Electoral Office, Estonia
Mikko Kolehmainen, Gofore
Marko Buuri, F-Secure

ESITYSLISTA

1 Kokouksen avaus

Varapuheenjohtaja Arto Jääskeläinen avasi kokouksen ja toivotti osallistujat sekä vieraat tervetulleiksi. Käytiin lyhyt esittäytymiskierros.

2 Edellisen kokouksen pöytäkirjan hyväksyminen

Hyväksyttiin muutoksitta.

3 e-Voting in Estonia

Tarvi Martens, Head of Internet Voting, State Electoral Office, Estonia

Tarvi Martens esitteli Viron nettiäänestysjärjestelmää, esitys liitteenä. Järjestelmä on ollut käytössä 8 vaaleissa 12 vuoden aikana. Järjestelmä on uudistettu ja sen tarkasteltavuutta sekä skaalautuvuutta on parannettu. Äänen salaamiseksi on erotettu äänen keräys (collector) ja käsittely (processor). Äänen sekoittamiseen käytetään homomorfaalista salausta (El Gamal). Kaikilla on salauksen ja päästä päähän todennettavuuden (end-to-end-verifiability) suhteen oma totuutensa ja kritiikkiä voidaan esittää. On harkittu sitä, että ei tarvitsisi ladata äänestyssovellusta, mutta käytännössä siitä ei ole aikomusta luopua. Uusi järjestelmä pohjautuu SQL:iin, aiemmin oli Python. Juhannukseen mennessä tehdään päätös siitä, otetaanko uusi järjestelmä käyttöön syksyn kunnallisvaaleissa. Elokuussa järjestelmään on tulossa julkinen kokeilu-aika.

Esityksen jälkeen käytiin läpi toimintamallia ja teknistä ratkaisua kyselemällä ja keskustelemalla.

Kysyttiin, mitä tapahtuu, jos mobiililaitteella tehtävässä äänen tarkistuksessa käy ilmi, että ääni on kirjautunut väärin. Jokaisella paikkakunnalla on päivystävä IT-asiantuntija niitä tilanteita varten. Ongelmia ei ole ollut kovin paljoa, mutta epäileviä äänestäjiä kehoitettaisiin äänestämään uudelleen toisella tietokoneella tai äänestyspaikalla.

Käyttöjärjestelmät, joille äänestyssovellus on ladattavissa ovat Windows, Mac and Linux. Digitaalinen allekirjoitus on keskeinen osa äänen suojaamista.

Paperiäänien ensisijaisuus varmennetaan siten, että lista netissä äänestäneistä ja ennakkooänet lähetetään äänestyspaikoille, missä tarkistetaan mahdolliset tuplääänestäneet. Ennen kuin nettiäänät lasketaan, merkitään tietojärjestelmään poistettavat nettiäänät.

Tunnistautuminen perustuu id-korttiin. Tästä nousi esille kysymys, voidaanko sähköinen id väärentää. Järjestelmä perustuu siihen, että id-korttiin voi ja tulee luottaa. Vain menemällä vaalipäivänä äänestyspaikalle voi tarkistaa, onko joku äänestänyt puolestasi väärennetyllä id:llä. Periaatteessa on siis mahdollista käyttää passiivisten äänestäjien digitaalisia allekirjoituksia. Tätä ei voida kuitenkaan tarkistaa.

Auditoinnin työkaluja ollaan kehittämässä mm. yhteistyössä yliopistojen kanssa ja sitä tehdään helpommaksi.

Jos havaitaan puutteita, laki antaa mahdollisuuden keskeyttää nettiäänestys. Nettiäänestystä ei voi käyttää enää vaalipäivänä, koska pitää olla mahdollisuus varajärjestelmään, jos nettiäänestyksessä on haavoittuvuuksia tai puutteita.

Tietoturvallisuutta tarkkaillaan ja tarkkailua helpottaa, että nettiäänestys on käytössä 7 päivän aikana. Valtion tietoturvaviranomainen tms. hoitaa nettiään. DDOS hyökkäys – voitaisiin esim. sulkea mahdollisuus käyttää järjestelmää ulkomailta vuorokaudeksi. Tietoturvauhista on raportti, joka uudistetaan ja julkaistaan parin kuukauden sisällä.

Näkemyks on että, vakaassa yhteiskunnassa ongelmia ei tule esim. vaalisalaisuuden suhteen.

4 Vaalitietojärjestelmä

Anniina Tjurin ja Juha Mäenalusta Oikeusrekisterikeskuksesta esittelivät käytössä olevaa vaalitietojärjestelmää.

Keskustelussa nousi esille, että järjestelmässä vaalien ylläpitäjien rooliin kiinnitettävä huomiota. Sähköinen vaaliluettelo keskeinen tutkijoiden näkökulmasta.

5 Hankkeen eteneminen

Projektipäällikkö Anneli Salomaa esitteli hankkeen tilanteen. Kansainvälisen vertailun vastauksista puuttuu vielä muutama ja lopullinen kooste saadaan seuraavaan kokoukseen mennessä. Riskityöpajoissa on keskeisten sidosryhmien kesken käyty läpi nettiäänestyksen riskejä. Näistä F-secure tekee koosteen, jota käytetään tietoturva vaatimusten määrittelyn pohjana.

6 Kuntaliiton puheenvuoro

Kuntaliiton edustaja Tommi Karttaavi esitteli tutkimustuloksia kansalaisten suhtautumisesta nettiäänestykseen ja Kuntaliiton näkemyksen.

7 Muut asiat

Ei muita asioita.

8 Seuraavat kokoukset

8.6.2017 klo 13.00-16.00 (pidennetty aika)

Tietoturvallisuus

29.8.2017 klo 13.00-15.00

Käytettävyys ja saavutettavuus, Jani Ruuskanen

9 Kokouksen päättäminen

Kokous päätettiin 15.00