

Sähköisen äänestyksen pilotin tietoturvaratkaisut

Vuoden 2008 kunnallisvaaleissa kolmen kunnan (Karkkila, Kauniainen ja Vihti) äänestäjät voivat valintansa mukaan äänestää joko sähköisesti äänestyspäätteellä tai äänestyslipulla. Kummassakin tapauksessa äänestäminen tapahtuu aiempien vaalien tapaan äänestyspaikalla vaaliviranomaisen valvonnassa. Etä-äänestys internetin välityksellä ei ole mahdollista.

Lainsäädäntö asettaa korkeat vaatimukset vaalien toimittamiselle ja käytettävien tietojärjestelmien luotettavalle toiminnalle. Sähköisen äänestysjärjestelmän tietoturvaratkaisun keskeiset osatekijät ovat:

- äänestyksen prosessi,
- järjestelmän käyttäjät ja näiden oikeudet,
- ohjelmistot,
- toimitilat, laitteet ja tietoliikenne sekä
- poikkeustilanteisiin varautuminen.

Äänestyksen prosessi

Vaalivirkailija tunnistaa äänestäjän henkilöllisyystodistuksen avulla. Vaalitoimitsija kirjaa äänestyksen alkaneeksi ja antaa äänestäjälle sähköisen äänestyskortin. Kortin avulla varmistetaan, että äänestäjä suorittaa äänestyksen äänestyspäätteellä äänioikeusrekisteriin tehdyn kirjauksen mukaisesti.

Järjestelmä salaa äänestäjän antaman äänen. Salaus tehdään äänestyspäätteessä välittömästi äänestäjän vahvistettua antamansa äänen. Salaus perustuu yleisesti käytössä olevaan julkisen avaimen menetelmään. Sen avulla varmistetaan vaalisalaisuuden säilyminen ja estetään äänestystuloksen selvittäminen ennen äänestyksen päättymistä.

Äänet säilytetään salatussa muodossa vaalien keskuslaitteistossa tarkasti valvotuissa tiloissa.

Äänten laskenta edellyttää, että paikalla on järjestelmän toimittajan lisäksi Helsingin vaalipiirilautakunnan ja Oikeusministeriön edustajista koostuva avausryhmä. Laskenta ei ole teknisesti mahdollista ilman näiden osapuolten läsnäoloa.

Järjestelmän käyttäjät ja näiden oikeudet

Järjestelmän käyttöoikeudet on tiukasti rajattu. Kullakin käyttäjällä on vain oman tehtävänsä edellyttämät oikeudet. Tärkeimmät oikeudet on lisäksi hajautettu. Yhdelläkään yksittäisellä henkilöllä tai intressiryhmällä ei ole sellaisia oikeuksia järjestelmässä, jotka mahdollistaisivat esimerkiksi vaalisalaisuuden murtamisen.

Ohjelmistot

Käytettävien ohjelmistojen oikeellinen toiminta varmistetaan kattavalla Oikeusministeriön ja tietotekniikkatoimittajan suorittamalla testauksella. Järjestelmä tarkastetaan ulkopuolisen tahon toimesta ja keskeisten ohjelmistojen muuttumattomuus varmistetaan vaalien aikana.

TietoEnator on järjestelmän tietotekniikkatoimittaja ja sen alihankkijana toimii espanjalainen sähköisen äänestyksen tietoturvaratkaisuihin erikoistunut yritys, Scytl Secure Voting S.A.

Toimitilat, laitteet ja tietoliikenne

Vaalitoimitsijat valvovat äänestyksen päätelaitteita vaalien aikana. Päätelaitteiden tekninen luotettavuus varmistetaan käynnistämällä ne vakiotilaan vaaleja varten suunnitellulta CD:ltä. Vakiotila rajaa päätelaitteen käytön äänestämiseen.

Palvelinlaitteet (keskuslaitteisto) sijaitsevat tarkasti valvotuissa tiloissa TietoEnatorin konesalissa Suomessa. Keskuslaitteisto on tärkeimpien komponenttien osalta kahdennettu. Yksittäisen palvelimen rikkoutuminen ei estä järjestelmän käyttöä.

Tietoliikenne pääte- ja palvelinlaitteiden välillä on suojattu käyttäen vahvoja, julkisia salausmenetelmiä ja muita hyväksi koettuja tietoturvaratkaisuja.

Äännet lasketaan laitteessa, joka ei ole yhteydessä tietoverkkoihin.

Poikkeustilanteisiin varautuminen

Vaaleissa varaudutaan myös mahdollisiin käyttökatkoihin (esim. sähkökatko). Tarvittaessa siirrytään varajärjestelyyn, jolloin äänestys jatkuu perinteisellä lippuäänestyksellä.