Sähköisen äänestyksen pilotti 2008

Tekninen toteutus ja tietoturvaratkaisut

Sähköisen äänestyksen pilotti 2008 - Tekninen toteutus ja tietoturvaratkaisut

1 Yleistä

Sähköisestä äänestyksestä on Suomessa säädetty vaalilaissa (880/2006). Sähköistä äänestystä tullaan pilotoimaan syksyllä 2008 järjestettävissä kunnallisvaaleissa. Pilotointiin osallistuvien kuntien (Karkkila, Kauniainen ja Vihti) äänestäjät voivat valintansa mukaan äänestää virallisessa äänestyspaikassa sähköisesti tai aiempien vaalien tapaan äänestyslipulla. Pilotointi ei vaikuta lippuäänestyksen vakiintuneisiin käytäntöihin.

Tässä dokumentissa kuvataan kunnallisvaaleissa 2008 käytettävän sähköisen äänestyksen järjestelmän tekninen ratkaisu. Dokumentti on suunnattu erityisesti tietotekniikan ammattilaisille, tietoturva-asiantuntijoille ja muille sähköisen äänestyksen tekniikoihin perehtyneille henkilöille.

Järjestelmän yleiskuva esitetään luvussa 2. Sähköisen äänestyksen prosessin vaiheet valmisteluista vaalituloksen laskentaan käydään läpi luvuissa 3 – 7. Luku 8 keskittyy sähköisten äänten salausratkaisuun. Luvussa 9 kuvataan lyhyesti vaalienaikaisia järjestelyjä. Luvussa 10 on lueteltu tärkeimpiä lähteitä, joista on saatavissa lisätietoja vuoden 2008 pilotointiin liittyen.

Dokumentissa keskitytään pilotin ohjelmistotekniseen toteutukseen ja tietoturvaratkaisuihin. Sähköisen äänestyksen tietoturvaan olennaisesti liittyviä tuotannonaikaisia järjestelyjä käsitellään vain lyhyesti.

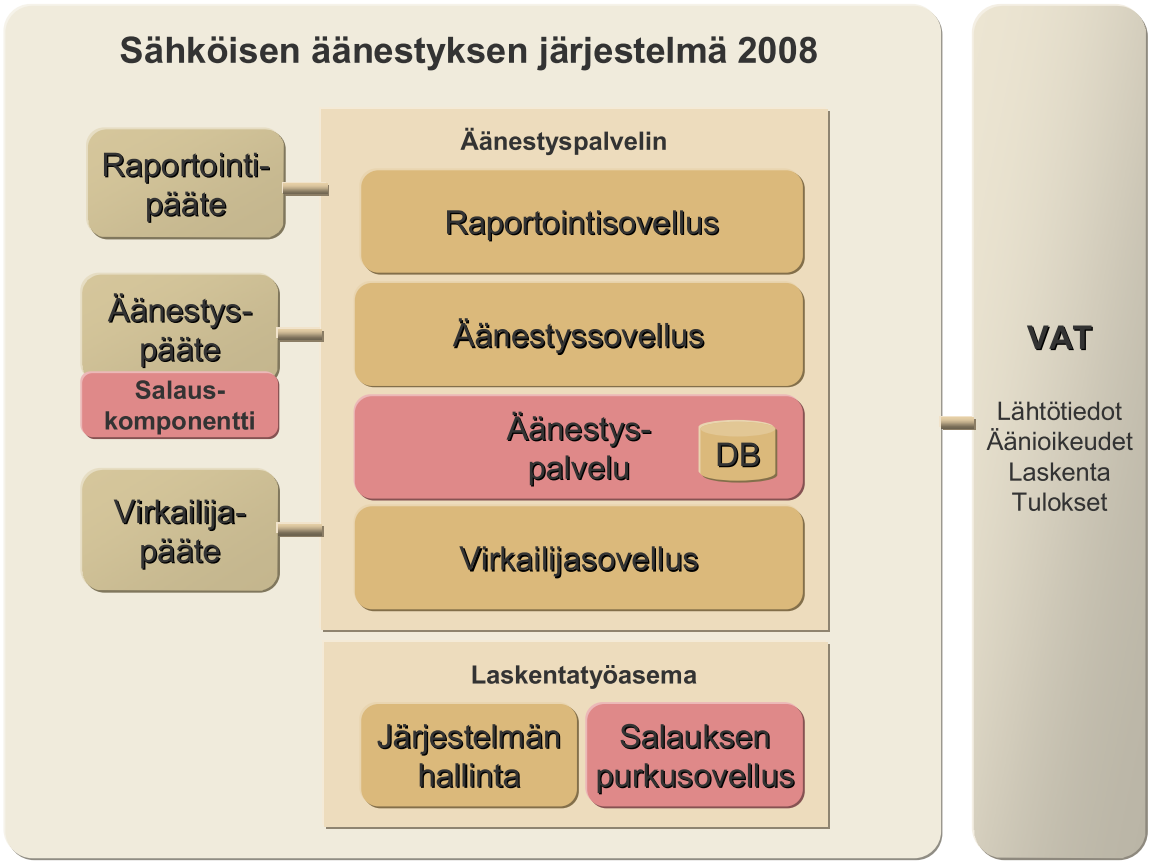
2 Yleiskuva järjestelmästä

Sähköinen äänestäminen tapahtuu äänestyspaikalla olevalla äänestyspäätteellä vaaliviranomaisten valvonnassa. Sähköisen äänestysjärjestelmän (kuva 1) toteutus perustuu sähköisen äänestyksen tietoturvaan keskittyneen Pnyx.core-tuotteen ja Suomessa pitkään käytössä olleen vaalitietojärjestelmän (VAT) integrointiin toimivaksi kokonaisuudeksi.

Vaalivirkailijat käyttävät *Virkailijan sovellusta* äänioikeuden tarkastamiseen ja äänestäjän äänioikeuden käytön kirjaamiseen.

Äänestäjä valitsee ehdokkaan *Äänestyssovelluksessa* ja vahvistaa tekemänsä valinnan, jonka jälkeen Äänestyssovellus salaa annetun äänen, allekirjoittaa sen sähköisesti ja lähettää sen Äänestyspalvelulle salattua tietoliikenneyhteyttä käyttäen.

Äänestyspalvelu tallentaa äänestäjän antaman äänen salatussa muodossa ja vahvistaa äänioikeuden käytön.



Kuva 1: Sähköisen äänestyksen järjestelmä

Vaaliviranomaiset käyttävät *Raportointisovellusta* sähköisen äänestyksen seurantaan. Sovelluksella voidaan vaalien aikana seurata sähköisesti äänestäneiden määrää ja vaalien päätyttyä sähköisen äänestyksen tuloslaskentaa.

Järjestelmän hallintaa käytetään sähköisen äänestyksen perustamiseen.

Salauksen purkusovelluksella poistetaan sähköisesti salattujen äänten ja äänestäjien tietojen välinen tekninen yhteys sekä puretaan äänten salaus. Tämä prosessi suoritetaan viranomaisten valvonnassa tietoverkoista erillään olevassa laiteympäristössä.

Vaalitietojärjestelmä (VAT) on keskuskoneella toimiva järjestelmä, jota käytetään mm. vaalien perustietojen ylläpitoon, äänten laskentaan ja vaalien tulospalveluun.

3 Vaalien valmistelu

Sähköisen äänestyksen valmisteluun liittyviä tehtäviä ovat mm. käytettävien ohjelmaversioiden tarkastus, perustietojen (äänioikeutetut, ehdokkaat, puolueet jne.) lataaminen VAT-järjestelmästä (turvallinen tiedostojen siirto) sekä sähköisen äänestysjärjestelmän konfigurointi.

Sähköinen äänestysjärjestelmä konfiguroidaan Helsingin vaalipiirilautakunnan ja Oikeusministeriön edustajien (ns. avausryhmän) läsnäollessa. Konfigurointi tehdään tietoverkoista erillään olevassa laitteessa.

Konfiguroinnin aikana luodaan kryptografiaan perustuva avainpari käyttäen julkisen avaimen (PKI) menetelmää. Avainparin yksityinen avain jaetaan osiin käyttäen ns. salaisen avaimen jakamisen menetelmää (secret sharing). Jokainen avausryhmän jäsen saa oman jaetun avaimen, joka tallennetaan avausryhmän jäsenen henkilökohtaiselle toimikortille. Toimikortti suojataan salasanalla, joka on ainoastaan kortin haltijan tiedossa. Tämän prosessin aikana alkuperäinen salainen avain tuhotaan, eikä se siten ole käytettävissä vaalien aikana.

Konfiguroinnissa luotua julkista avainta käytetään myöhemmin äänestyksessä. Sen avulla salataan jokainen annettu sähköinen ääni. Sähköiseen äänestysjärjestelmään tallennetut äänet voidaan purkaa ainoastaan edellä mainitun avausryhmän toimesta. Tämä tapahtuu siten, että Helsingin vaalipiirilautakunnan ja Oikeusministeriön edustajat luovuttavat hallussaan olevat jaetut avaimet ja näiden yhdistelmällä luodaan uudelleen salauksessa käytettyä julkista avainta vastaava yksityinen avain. Tämä prosessi (mixing protocol) on kuvattu tarkemmin luvussa 8.

4 Äänioikeuden tarkastus ja käytön kirjaaminen

Vaalivirkailija tunnistaa äänestäjän henkilöllisyystodistuksen avulla perinteisen lippuäänestyksen tapaan. Virkailija kirjaa äänestyksen alkaneeksi ja antaa äänestäjälle sähköisen äänestyskortin (toimikortti), jonka avulla äänestäjä voi antaa yhden äänen.

Virkailijan sovelluksella vaalivirkailijat

- tarkastavat äänestäjän äänioikeuden VAT-järjestelmästä,
- kirjaavat äänestyksen alkaneeksi VAT-järjestelmään ja
- luovat äänestäjälle sähköisen äänestyskortin.

Virkailijan sovellus kirjaa äänestyksessä tarvittavat äänestäjän tiedot sähköiselle äänestyskortille (valmistaja Giesecke Devrient). Kortin avulla varmistetaan, että äänestäjä suorittaa äänestyksen äänestyspäätteellä äänioikeusrekisteriin tehdyn kirjauksen mukaisesti.

Virkailijan päätelaite on standardi PC, joka käynnistetään turvalliseksi varmistetulta kertakirjoitettavalla medialla (CD/DVD). Ratkaisulla estetään haittaohjelmien toiminta ja rajataan päätelaitteen käyttö sähköisen äänestyksen järjestelmään. Päätelaitteen yhteydessä on kortinlukija (valmistaja OmniKey), jota käytetään sähköisen äänestyskortin (Smart Card) hallintaan.

Virkailijan sovellus koostuu selainkäyttöliittymästä ja palvelinsovelluksesta. Firefox-selaimella toimiva käyttöliittymä on toteutettu JSP-sivuina. Sähköisten äänestyskorttien käsittelyyn käytetään JavaScript- ja Applet-teknologioita. Palvelinsovellus on toteutettu J2EE-tekniikalla ja se on reaaliaikaisessa yhteydessä äänestyspalvelimeen ja VAT-järjestelmään JDBC-tekniikalla.

5 Äänestäminen

Äänestäminen tapahtuu äänestyskopissa olevalla äänestyspäätteellä. Äänestyspäätteen käyttäminen edellyttää, että äänestäjällä on käytössään virkailijalta saatu sähköinen äänestyskortti. Järjestelmä varmistaa, että äänestäjä voi antaa yhden ja vain yhden äänen.

Äänestäjän vastaanotettua äänestyskortti, hän

- kirjautuu järjestelmään syöttämällä sähköisen äänestyskortin lukijaan,
- valitsee ehdokkaan syöttämällä ehdokasnumeron,
- vahvistaa tekemänsä äänestysvalinnan ja
- palauttaa sähköisen äänestyskortin vaalivirkailijalle.

Äänestyksen yhteydessä äänestäjän sovellus

- tarkistaa äänestyskortin tietojen oikeellisuuden,
- tarkistaa äänestäjän äänioikeuden äänioikeusrekisteristä (VAT),
- tarkistaa virkailijan kirjaaman äänestyksen aloitusmerkinnän
- salaa ja allekirjoittaa äänestäjän antaman äänen sähköisesti,
- merkitsee äänioikeuden käytetyksi ja
- tallentaa salatun äänen äänestyspalvelimelle.

Äänestäjän päätelaite on kosketusnäytöllä ja kortinlukijalla varustettu standardi PC, joka käynnistetään virkailijan päätelaitteen tapaan kertakirjoitettavalla medialla. Kosketusnäyttö rajaa äänestyspäätteen käytön äänestyskäyttöliittymän toimintoihin.

Äänestäjän sovellus koostuu käyttöliittymästä ja palvelinsovelluksesta. Käyttöliittymä on toteutettu Java-sovelluksena ja sen toiminnallisuus perustuu Swing-teknologiaan. Käyttöliittymä välittää äänestäjän tunnistamiseen ja äänestystapahtumaan liittyvät pyynnöt salattuina äänestyspalvelimella sijaitsevalle äänestyspalvelulle.

Keskitetyllä *äänestyspalvelimella on* äänestyspalvelu (Pnyx.Core) ja tietovarasto (Oracle DB). Äänestyspalvelu ottaa äänestyssovelluksen salaaman äänen vastaan (Ballot Casting Protocol), tarkistaa äänestäjän äänioikeuden, vahvistaa äänioikeuden käytön VAT-järjestelmän äänioikeusrekisteriin ja tallentaa käyttöliittymän lähettämän salatun äänen tietovarastoon. Käytetty salausratkaisu varmistaa vaalisalaisuuden säilymisen ja estää äänestystuloksen selvittämisen ennen äänestyksen päättymistä. Tietovaraston eheys varmistetaan mm. kryptografisesti varmennetuilla lokitiedoilla.

6 Salauksen purku ja laskenta

Sähköisesti annettujen äänten salaus puretaan vaalien päätyttyä tietoverkoista erillään olevassa laitteessa, johon äänet siirretään fyysistä mediaa käyttäen (esim. CD-ROM). Salauksen purku tehdään Helsingin vaalipiirilautakunnan ja Oikeusministeriön edustajien (avausryhmän) toimesta. Kukin edustaja luovuttaa hallussaan olevan jaetun avaimen salauksen purkusovellukselle. Tämä tapahtuu siten, että kukin edustaja kirjautuu järjestelmään käyttäen hallussaan olevaa toimikorttia ja salasanaa. Järjestelmä muodostaa jaettujen avainten avulla sähköisen äänestyksen salaisen avaimen, jonka avulla äänten salaus on purettavissa.

Salauksen purkusovellus suorittama prosessi purkaa äänten salauksen samalla sekoittaen annettujen äänten järjestyksen. Tämä poistaa mahdollisuuden yhdistää purettu ääni sen antaneeseen äänestäjään sen perusteella missä järjestyksessä äänestys on tapahtunut. Tämä prosessi on kuvattu tarkemmin luvussa 8

Salauksen purkusovellus laskee sähköisesti annetut äänet yhteen ja tarvittaessa yhdistää tulokset laissa (vaalilaki 86a§) säädettyjen ehtojen mukaisesti.

7 Sähköisten äänten yhdistäminen lippuääniin ja vaalituloksen laskenta

Vaalitietojärjestelmä (VAT) on keskuskoneella (IBM-mainframe, DB2 ja IDMS) toimiva järjestelmä, jota on käytetetty Suomessa useita vuosia yleisten vaalien järjestämisessä. Järjestelmää käytetään vaalien perustietojen (puolueet, ehdokkaat, äänioikeutetut jne.) ylläpitoon, lippuäänten kirjaukseen, äänten laskentaan (ml. lippuäänet ja sähköiset äänet) sekä vaalien tulospalveluun.

Sähköisesti annettujen äänten laskennan tulokset siirretään VAT-järjestelmään. VAT-järjestelmä yhdistää sähköiset äänet lippuääniin, jonka jälkeen suoritetaan varsinainen vaalituloksen laskenta. Vaalitulos välitetään VAT-järjestelmästä vaaliviranomaisille, tiedotusvälineille ja muille sidosryhmille.

8 Äänten salaus

Sähköisen äänestysjärjestelmän salaus on toteutettu erikseen tietoliikenteen ja sovelluksen tasoilla. *Tietoliikenneyhteydet* salataan yleisesti käytetyllä SSL-salausprotokollalla.

Äänten salaus perustuu *sovelluksen tasolla* Pnyx.core-tuotteen tietoturvaratkaisuihin. Pnyx.core on turvalliseen sähköiseen äänestykseen erikoistuneen yhtiön (Scytl Secure Electronic Voting, S.A.) kehittämä ja ylläpitämä tuote. Tuotteen keskeiset osat ovat: Voting Client (äänestyspäätteen salauskomponentti), Voting Proxy ja Voting Service (äänestyspalvelu) sekä Mixing Service (salauksen purkusovellus). Pnyx.coren toiminta perustuu ohjelmiston sisäisten protokollien käyttöön, joista tärkeimmät ovat äänestysprotokolla ja salauksen purkuprotokolla.

Äänestysprotokolla (Ballot Casting Protocol) käsittää äänestystapahtumaan liittyvät toiminnot. Äänestäjä syöttää valitsemansa ehdokasnumeron kosketusnäytöllä, jonka jälkeen järjestelmä näyttää numeroa vastaavan ehdokkaan tiedot ja pyytää äänestäjää vahvistamaan valintansa. Vahvistuksen jälkeen annettu ääni mukaan lukien tieto kunnasta ja äänestyspaikasta salataan äänestyspäätteessä käyttäen avausryhmän julkista avainta ja tallennetaan keskitetylle äänestyspalvelimelle. Tehty salaus on purettavissa ainoastaan yksityisellä avaimella, joka on kryptografisesti jaettu ja jonka osat ovat avausryhmän jäsenten hallussa olevilla henkilökohtaisilla ja salasanalla suojatuilla toimikorteilla.

Äänten sovellustasolla tehtävässä salauksessa käytetään yleistä julkisen avaimen (PKI) menetelmää. Äänten salaus perustuu julkisen ja salaisen avaimen muodostamaan avainpariin, joiden välillä on matemaattinen riippuvuus. Julkisella avaimella salattu tieto on selvitettävissä ainoastaan sitä vastaavan salaisen avaimen avulla. Sähköisen

äänestysjärjestelmän tapauksessa salainen avain ei ole minkään yksittäisen tahon hallussa, vaan se on jaettu kullekin avausryhmän jäsenelle kryptografista algoritmia (secret sharing) käyttäen. Koska salainen avain tuhotaan jakoprosessin aikana, se voidaan muodostaa vain avausryhmän jäsenten hallussa olevien jaettujen avainten yhdistelmällä.

Salauksen purkuprotokolla (Mixing Protocol) suoritetaan äänestyksen päätyttyä ennen varsinaista äänten laskentaa. Salauksen purku tapahtuu tietoverkoista irti olevassa tietokoneessa. Avausryhmän jäsenet muodostavat äänestyksen salaisen avaimen käyttäen hallussaan olevia henkilökohtaisia toimikortteja ja salasanoja. Salauksen purkuprotokolla muodostaa äänten salauksessa käytettyä julkista avainta vastaavan salaisen avaimen, jonka jälkeen yksittäisten äänten oikeellisuus tarkistetaan ohjelmallisesti ja niiden salaus puretaan. Salauksen purkamisen yhteydessä äänten järjestys muutetaan ohjelmallisesti satunnaiseksi siten, ettei yksittäisen äänen antajaa voida selvittää esimerkiksi äänestyksen ajankohdan perusteella.

Tärkeimmät järjestelmässä käytetyt PKI-standardit ovat x.509v3 (varmenteet), PKCS (salaus, Public Key Cryptography Standards) ja CRL (sulkulista, Certificate Revocation List).

9 Laadunvarmistus ja vaalien aikaiset järjestelyt

Pilotin *laadunvarmistus* käsittää mm. järjestelmän kattavan testauksen ja ulkopuolisen tahon suorittaman tarkastuksen. Järjestelmän osien muuttumattomuus varmistetaan sähköisillä allekirjoituksilla ja käytön aikana mm. käyttöliittymän varmenteen (Code Signing Certificate) automaattisella tarkistuksella.

Vaalien aikaisilla järjestelyillä on keskeinen merkitys sähköisen äänestyksen luotettavuuden varmistamisessa. Tärkeitä osa-alueita ovat vaalivirkailijoiden toiminta (esim. äänestyspaikkojen valvonta), fyysinen tietoturva (esim. päätelaitteiden fyysinen suojaus), käyttöoikeudet ja pääsynvalvonta sekä tietoliikenteen suojaus.

Vaalien ajaksi laaditaan myös varasuunnitelma poikkeustilanteiden varalle. Esimerkiksi mahdollinen sähkökatko voidaan hoitaa eri tavoin mukaan lukien siirtyminen varajärjestelyyn tietyllä rajatulla alueella, jolloin äänestys jatkuu perinteisellä lippuäänestyksellä.

10 Lisätietoja

Laki vaalilain muuttamisesta (880/2006) www.finlex.fi.

Sähköisen äänestyksen järjestelmän toimittaa TietoEnator www.tietoenator.fi. TietoEnator on toimittanut tietojärjestelmäpalveluja Suomen kansallisiin vaaleihin 80-luvun puolivälistä alkaen.

Tarkemmat kuvaukset Pnyx.core-tuotteesta löytyvät valmistajan Internet-sivuilla osoitteessa www.scytl.com.

Lisätietoja sähköisen äänestyksen pilotista antaa Oikeusministeriö.