SÄHKÖINEN ÄÄNESTÄMINEN 2008

Sähköisen äänestämisen kokeilu kunnallisvaaleissa 2008

Äänestysjärjestelmän tekninen esittely

Tekniset lähtökohdat

- Keskitetty äänestysjärjestelmä:
  - Sähköisen äänestyksen keskitetty palvelinjärjestelmä, jonka ohjelmisto ja tietovarasto muodostavat ns. sähköisen uurnan
  - Äänestyspäätteet ovat tietoliikenneverkon kautta yhteydessä keskitettyyn palvelinjärjestelmään
- Työasemissa normaali PC-teknologia
- Ei paperitulostetta
- Sähköisen äänestyksen tietoturva ja vaalisalaisuus varmistettu käyttäen pitkälle kehitettyjä salausmenetelmiä
- Teknisiä tietoturvaratkaisuja täydennetään roolien jakamisella
  - Vaalivirkailijat: toiminta äänestyspaikalla
  - Sähköisen uurnan avausryhmä: äänten salauksen purkaminen
  - Tekninen hallintaryhmä: vaalien konfiguraatiotiedot
- Sähköinen äänestys ja perinteinen lippuäänestys käytössä rinnakkain
- Käytössä kaksi tietojärjestelmää:
  - Sähköisen äänestyksen järjestelmä
  - Pitkään käytössä ollut vaalitietojärjestelmä (VAT/uVAT)
- VAT-järjestelmällä huolehditaan ennakkoäänestyksessä muiden kuin sähköisesti äänestävien äänioikeuden tarkastus ja käytön merkitseminen
- Rinnakkaisen käytön mahdollistamiseksi järjestelmät integroitu:
  - Virallinen äänioikeusrekisteri VAT-järjestelmässä
  - Sähköisessä äänestysjärjestelmässä kopiona äänioikeusrekisterin osajoukko eli pilottikuntien äänestäjät
  - Sähköisessä äänestyksessä äänioikeus tarkastetaan ja merkitään käytetyksi molempiin järjestelmiin
  - Äänioikeuden käyttö näkyy välittömästi molemmissa järjestelmissä

Lyhyt katsaus pilotin tietoturvaratkaisuihin

- Äänestyksen prosessi
  - Vaalivirkailija tunnistaa äänestäjän henkilöllisyyden
  - Äänet säilytetään salatussa muodossa. Laskenta edellyttää ns. avausryhmää.

- Järjestelmän käyttäjät ja näiden oikeudet
  - Järjestelmän käyttöoikeudet on tiukasti rajattu
  - Mikään taho ei yksin kykene esim. murtamaan vaalisalaisuutta

- Ohjelmistot
  - Pitkälle kehitetyt salausmenetelmät
  - Testaus ja 3. osapuolen suorittama auditointi
  - Muuttumattomuus vaalien aikana varmistetaan teknisesti

- Toimitilat, laitteet ja tietoliikenne
  - Päätelaitteita käytetään vakiotilassa ja vaalivirkailijoiden valvonnassa
  - Palvelimet sijaitsevat valvotuissa tiloissa ja laitteet kahdennettuina
  - Tietoliikenne pääte- ja palvelinlaitteiden välillä on salattu

- Poikkeustilanteisiin varautuminen
  - Tarvittaessa (esim. sähkökatko) siirrytään lippuäänestykseen

Vaalien perustaminen – tekniset toimenpiteet

- Pilotin tuotantoympäristö asennetaan ennen vaalin perustamista
  - Laitteet, ohjelmistot ja tietoliikenne
  - Perustietojen siirtäminen vaalitietojärjestelmästä Pnyx.Core-tuotteelle
    - Äänioikeutetut, ehdokkaat, äänestysalueet ja -paikat
    - Ehdokasluettelo äänestyssovellukselle XML-muodossa
    - PKCS#12-tunnisteiden muodostus äänestäjiä varten
  - Järjestelmän käyttäjäryhmät ja näiden käyttöoikeudet

- Perustaminen tapahtuu valvotusti
  - Helsingin vaalipiirilautakunnan ja oikeusministeriön edustajista koostuva avausryhmä
  - Ryhmä valvoo myös sähköisten äänten laskentaa, kuten vaalilaissa on säädetty

- Kaikki keskeiset tietoturvatoiminnot suoritetaan laskentatyöasemalla, jota ei kytketä tietoverkkoon

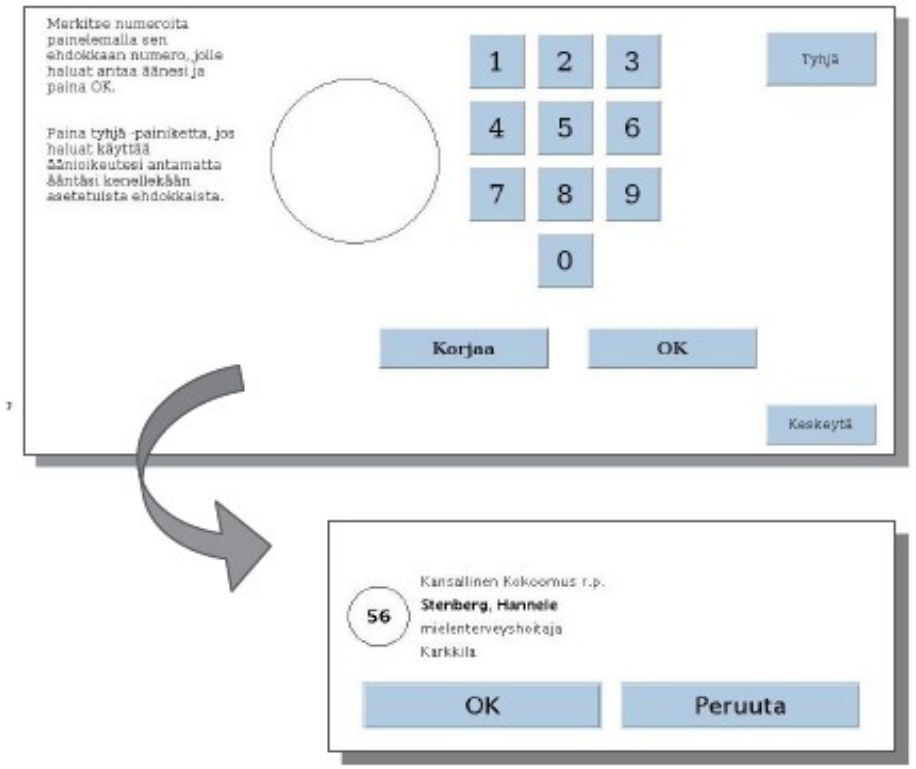
1. Määritellään sähköisen äänestyksen lähtötiedot järjestelmään
   - Aloitus ja lopetusajankohta, sähköisten äänten salauksen purkamiseen käytettävien toimikorttien lukumäärä, jne
2. Avausryhmän jäsenet luovat äänten salauksen purkuun käytettävät toimikortit
   - Jäsenet syöttävät vuorollaan toimikortin lukijaan ja määräävät toimikortille salasanan
3. Otetaan käyttöön luodut määritykset
   - Siirretään pilotin konfiguraatiot palvelinlaitteelle

Äänestys sähköisesti - virkailijan toiminta

- Virkailija tarkastaa äänestäjän henkilöllisyyden ja äänioikeuden.
- Äänestäjän valitessa sähköisen äänestyksen, virkailija syöttää tilapäisen sähköisen äänestyskortin kortinlukijaan.
- Virkailija tallentaa äänestyksessä tarvittavat tiedot kortille ja kirjaa äänioikeuden käytetyksi.
- Virkailija luovuttaa sähköisen äänestyskortin äänestäjälle

Äänestys sähköisesti - äänestäjän toiminta

- Äänestäjä menee äänestyskoppiin.
- Äänestäjä syöttää sähköisen äänestyskortin kortinlukijaan.
- Äänestäjä tarkistaa ehdokkaan numeron äänestyskopin seinältä.
- Valitsee ehdokkaan numeron äänestyspäätteen kosketusnäytöllä
- Äänestäjä vahvistaa tekemänsä valinnan, jolloin ääni kirjataan järjestelmään ja äänioikeuden käyttö vahvistetaan.
- Äänestäjä ottaa äänestyskortin pois lukijasta ja palauttaa kortin.



Sähköisen äänestysjärjestelmän keskeiset komponentit

Järjestelmän rakenne ja tekniset ratkaisut

Java-sovellus:
- Swing-käyttöliittymä
- WebStart-käynnistys
- Java-kirjastot: salaus- ja korttitoiminnot

Äänestyspääte

https

https

Pnyx-vp

- WebLogic
- Pnyx.Core
- Oracle-tietokanta

Sähköinen uurna

Palvelimessa ei verkkoyhteyttä

Kts. sähköinen uurna

Laskentatyöasema

Selain pohjainen:
- HTML
- JavaScript
- Java-Applet: korttitoiminnot

Virkailijan pääte

https

Mainframe
DB2-tietokanta

Vaalitietojärjestelmä (VAT)

Pnyx-vp = Pnyx.Core Voting Protocol (sisältää mm. äänen salauksen)

Keskeiset salaustekniikat

- Äänten käsittely vaalien aikana:
  - Äänestysprotokolla (Ballot Casting Protocol, Pnyx.Core)
  - Salauksen purkuprotokolla (Mixing Protocol, Pnyx.Core)
- Äänestäjien tunnistus
  - PKCS#12 (Personal Information Exchange Syntax Standard)
- Äänten ja konfiguraatiotietojen salaus
  - Public Key Cryptography
  - Secret sharing
- Tietoliikenteen salaus
  - HTTPS/SSL-protokolla + client-sertifikaatit
- Työaseman suojaus ja vakionti
  - Knoppix-käyttöjärjestelmä, käynnistys CD/DVD-levyltä

Vaalituloksen laskenta

1.Laskenta aloitetaan vaalipäivän äänestyksen päätyttyä. Sähköisestä uurnasta tuotetaan salatut äänet sisältävä XML-tiedosto, joka kopioidaan laskentatyöasemalle (säilytetty kassakaapissa)

2. Avausryhmän edustajat kirjautuvat järjestelmään toimikorteillaan. Äänten salaus puretaan laskentatyöasemalla avausryhmän hallussa olevaa jaettua yksityistä avainta käyttäen

3. Lisäksi salauksen purkamisen yhteydessä
– Sekoitetaan äänten järjestys vaalisalaisuuden varmistamiseksi
– Varmistetaan äänten oikeellisuus vertaamalla laskenta-työasemalla vaalien ajan säilytettyihin tietoihin (mm. Äänioikeutetut)

4. Selväkieliset äänet summataan ehdokkaittain ja äänestysalueittain

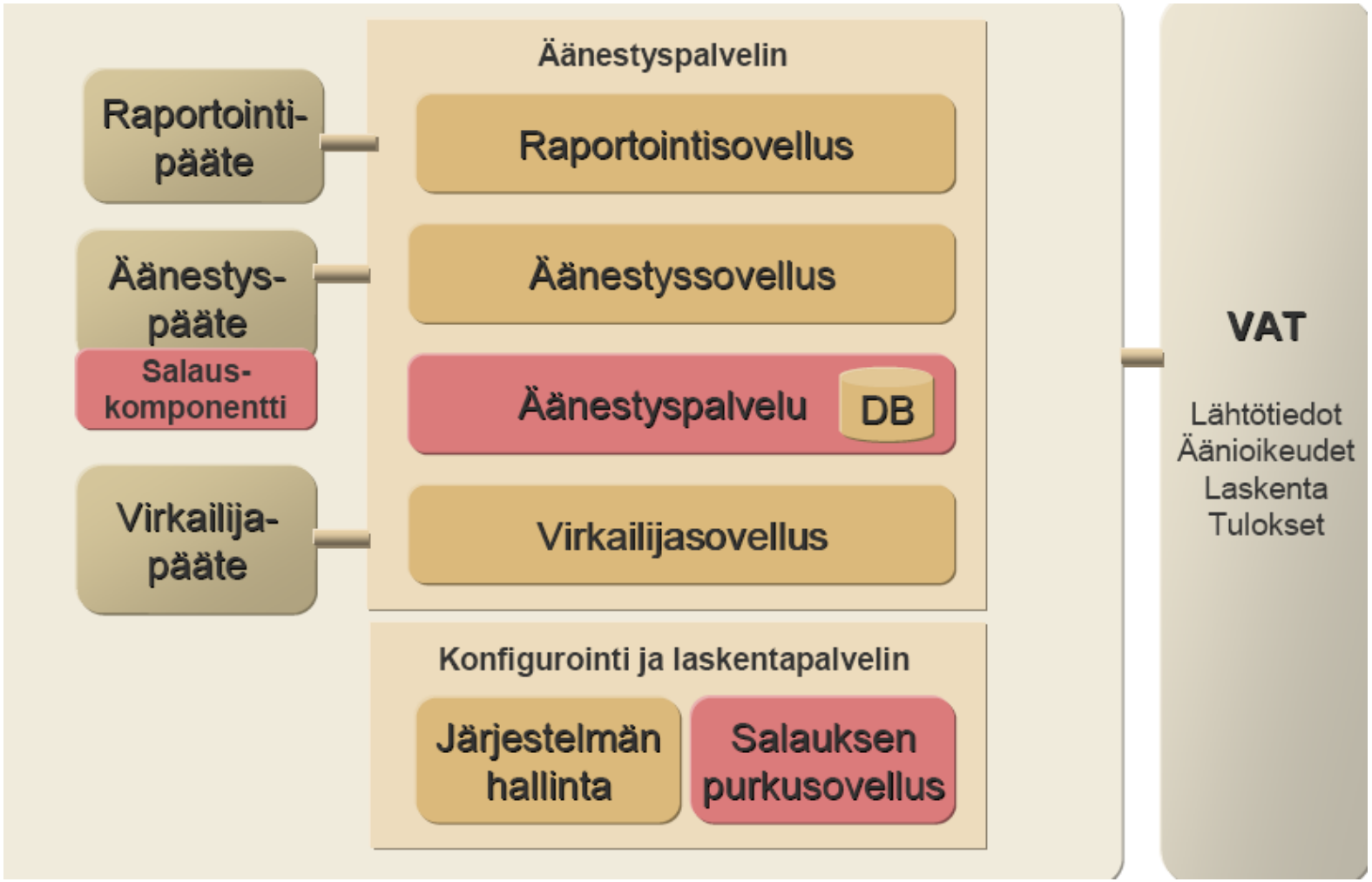
5. Tarvittaessa äänet yhdistetään vaalilain (86a§) mukaisesti

6. Sähköiset äänimäärät siirretään vaalitietojärjestelmään, jossa ne yhdistetään lippuääniin ja huomioidaan lopullisissa vaalituloksissa

7. Vaalin tulos välitetään viranomaisille ja medialle

”Vaalipäivän äänestyksen päätyttyä sähköisen vaaliuurnan avaavat ja uurnassa olevat äänet laskevat yhdessä ja samanaikaisesti Helsingin vaalipiirilautakunnan puheenjohtaja tai varapuheenjohtaja ja kaksi muuta jäsentä sekä oikeusministeriön edustaja.”

Sähköisen äänestyksen järjestelmä 2008



Laadunvarmistus projektin eri vaiheissa

- Tuotteiden laadunvarmistus
  - Tuotetoimittajien sisäinen laadunvarmistus
  - Keskeisten tuotteiden vastaanottotarkastukset
- Testaukset ja kenraaliharjoitukset
  - TietoEnatorin toteuttamien ohjelmistojen komponenttitestaus
  - Järjestelmätestaus pilotille
  - Hyväksymistestaus
  - Käyttöönotto- ja suorituskykytestaus tuotantoympäristössä
  - Kenraaliharjoitukset
- Ulkopuolisten asiantuntijoiden suorittamat tarkastukset
  - Toteutuksen ja toimintaprosessien auditointi 3. osapuolen toimesta
  - Mahdollinen ulkomaisten vaalitarkkailijoiden suorittama arviointi
- Vaaliorganisaation suorittamat tarkastukset
  - Käyttöönottotarkastus ennen vaaleja ja säännölliset tarkistukset
  - Ympäristön tarkastus vaalien päätyttyä

Sähköisen äänestysjärjestelmän toimittajat

Sähköisen äänestysjärjestelmän toimittaa TietoEnator Oyj. Järjestelmän tietoturvaratkaisu tukeutuu espanjalaisen SCYTL Secure Electronic Voting S.A:n kehittämään Pnyx.core -tuotteeseen.

TietoEnator

- Tausta
  - Yksi Euroopan suurimpia tietotekniikan palveluyrityksiä
  - Vuotuinen liikevaihto yli 1.6 miljardia euroa
  - Työntekijöitä n. 16.000, joista n 1.000 valtiosektorin parissa
  - Yli 40 vuoden kokemus tietotekniikkapalvelujen toimittajana

- Sijainti
  - Pääkonttori Espoossa
  - Toimipisteitä lähes 30 maassa

- Omistajat
  - Osakkeet noteerataan Tukholman ja Helsingin pörsseissä

- Toiminta vaalien tietotekniikkatoimittajana
  - Vaaleihin liittyvien palvelujen tuottaja yli 20 vuoden ajan
  - Suomessa nykyisin käytetyn vaalitietojärjestelmän (VAT) toteuttaja

Scytl – Secure Electronic Voting

- Tausta
  - Sovellustason kryptografiaan erikoistunut ohjelmistoyritys
  - Perustettu vuonna 2001 akateemisen tutkimusryhmän yhtiöittämisellä
  - Yksi johtavista sähköisen äänestämisen ratkaisutoimittajista maailmassa
- Sijainti
  - Pääkonttori Barcelonassa
  - Toimistot Yhdysvalloissa ja Singaporessa
- Omistajat
  - Spinnaker, pääomarahasto, Espanja
  - Nauta, pääomarahasto, Espanja
  - Yrityksen johto ja perustajat
- Tuotteet
  - Tietoturvaratkaisu: Pnyx.core
  - Toimialakohtaisia tuotteita: Pnyx.labour, Pnyx.corporate, Pnyx.government, Pnyx.DRE, Pnyx.VM, Pnyx.VVPAT, PressVote and Election Management Systems

Scytlin salausprotokolla on suojattu kansainvälisillä patenteilla

-

Spanish Patent & Trademark Office
U.S. Patent Office

Ratkaisut ovat saaneet useita kansainvälisiä palkintoja (mm. Euroopan komissio 2005)

-

IST, information society technology
www.ict-prize.org

Scytl S.A. – referenssejä

Commision on Elections **Philippines**	Tradenomiliitto **Finland**
Department of Constitutional Affairs **United Kingdom**	Canton of Neuchâtel **Switzerland**
Victorian Electoral Commision **Australia**	Parliament of Nuevo Leon **Mexico**
Government of Mendoza **Argentina**	Parliament of Catalonia **Spain**