Nettiäänestyksen esiselvitys

Versio 1.0

- Johdanto
- Järjestelmän toiminnallisuus
- Järjestelmävaatimukset
- Tietoturvallisuus
  - Tietoturvallisuuden ja varautumisen taso
  - Lisävaatimukset tietoturvallisuuden osalta
  - Jäljelle jäävät uhat
- Kustannus- ja hyötyanalyysi
  - Hyötyjä
  - Kustannukset
  - Kustannustekijöitä
  - Vaihtoehtoiset toteutukset
- Laatutavoitteet
- Integrointi muihin järjestelmiin
  - Vaalitietojärjestelmä (VAT)
  - Väestötietojärjestelmä (VTJ)
  - VETUMA
  - Operointijärjestelmät
  - Monitorointi
  - Äänestäjän päätelaitteet
- Kilpailutuksen perusteet ja markkinakartoitus
- Suunnitelma toteutus- ja käyttöönottovaiheelle
- Yhteenveto
- Liite 1: Työpajoihin osallistuneet

CODENTO

Johdanto

Oikeusministeriön koordinoima Osallistumisympäristö-hanke, joka kuuluu SADe-ohjelmaan, antoi Codenton tehtäväksi laatia esiselvityksen nettiäänestyksen käyttämisestä kunnallisten neuvoa-antavien kansanäänestysten toteuttamisessa. Codento järjesti yhdessä nettiäänestystyöryhmän ja muiden esiselvityksen työstämiseen nimettyjen tahojen kanssa kolme työpajaa nettiäänestykseen liittyvistä proseduraalisista ja teknisistä vaatimuksista, ongelmista ja reunaehdoista. Työpajojen lisäksi nettiäänestystyöryhmä, muut työhön osallistuneet asiantuntijat ja Codenton konsultit ovat keskustelleet tämän dokumentin luonnoksista kahdesti. Tämä dokumentti kuvaa työpajojen ja keskusteluiden aikana syntyneen käsityksen kunnallisten neuvoa-antavien kansanäänestysten toteuttamisesta yleisessä internetissä äänestäjien omia päätelaitteita käyttäen. Tätä kutsutaan nettiäänestykseksi.

Dokumentti käsittelee kansanäänestystä ratkaisulähtöisesti. Nettiäänestykseen yleisesti ja erityisesti kunnallisiin neuvoa-antaviin kansanäänestyksiin liittyvien ongelmien lisäksi tuodaan esille ongelmiin nähtävissä olevia teknisiä ja lainsäädännöllisiä ratkaisuja.

Nettiäänestystyöryhmä on myös keskustelut yleisten vaalien järjestämisestä netin kautta. Yleiset vaalit eivät kuitenkaan olleet tämän toimeksiannon keskiössä. Tästä syystä vaaleihin liittyvät ongelmat, ratkaisut ja huomiot on tässä dokumentissa erotettu kansanäänestykseen liittyvistä. Erottaminen on tehty niin, että vaaleihin liittyvä teksti on kirjoitettu kursiivilla.

Kunnallisesta neuvoa-antavaa kansanäänestystä (jatkossa “kansanäänestys”) säätelee laki “Laki neuvoa-antavissa kunnallisissa kansanäänestyksissä noudatettavasta menettelystä” vuodelta 1990[1]. Äänestykseen voi osallistua äänestyspäivänä äänestyspaikalla ja ennakkoon kirjeäänestyksenä. Lain mukaan

> keskusvaalilautakunta lähettää viimeistään 19. päivänä ennen äänestyspäivää jokaiselle äänestysoikeutetulle, jonka osoite on tiedossa, 3 §:ssä tarkoitetussa päätöksessä käytettäväksi määrätyt äänestysliput, vaalikuoren, lähetekirjeen, lähetekuoren ja laatimansa äänestysohjeet (kirjeäänestysasiakirjat).

Äänestäjä puolestaan lain mukaisesti toimiessaan ja äänestäessään

[1] http://www.finlex.fi/fi/laki/ajantasa/1990/19900656

> Tehtyään äänestysmerkinnän äänestysoikeutetun tulee sulkea äänestyslippu tai, jos niitä on käytettävissä useampia, valitsemansa äänestyslippu vaalikuoreen, täyttää ja omakätisesti allekirjoittaa lähetekirje, sulkea vaalikuori ja lähetekirje lähetekuoreen ja lähettää lähetekuori postitse kunnan keskusvaalilautakunnalle siten, että se saapuu sille viimeistään äänestyspäivää edeltävänä perjantaina kello 19.

Nettiäänestyksen tarkoitus on korvata tämä kirjeäänestys kokonaan tai mahdollisimman laajasti. Kirjeäänestykselle laissa säädetyt määräajat ovat niin tiukat, että suuret kaupungit eivät käytännössä kykene järjestämään kansanäänestyksiä. Nettiäänestys todennäköisesti vähentäisi kirjeäänestyshalukkuutta, mikä tarkoittaisi suurillekin kunnille parempia mahdollisuuksia järjestää kunnallisia kansanäänestyksiä luotettavasti ja matalammin kustannuksin.

Tämä dokumentti kertoo ensin nettiäänestysjärjestelmän toiminnallisuudet. Koska nettiäänestystä säätelevää lainsäädäntöä ei vielä ole olemassa, dokumentissa määritellään osittain myös teknisten ratkaisujen lainsäädännölle asettamia reunaehtoja.

Dokumentti esittelee kansanäänestyksiin soveltuvan nettiäänestysjärjestelmän perusperiaatteet ja toiminnan. Järjestelmän toiminnallisuudet esitetään yksinkertaisesti ja ymmärrettävästi, jotta dokumentin ymmärtäminen ei vaadi syvällistä tietoteknistä osaamista. Nettiäänestysjärjestelmän ymmärrettävyys on edellytys sen hyväksynnälle ja käytön laajenemiselle.

Seuraavaksi dokumentissa verrataan nettiäänestysjärjestelmän toiminnallisuuksia ja ominaisuuksia yleisiin nettiäänestysjärjestelmille asetettuihin vaatimuksiin. Osa vaatimuksista pätee vain vaaleissa. Eräiden vaatimusten ei tarvitse päteä nettiäänestyksessä, koska ne eivät päde nykyisessäkään kirjeäänestyksessä eivätkä nykymuotoisessa ennakkoäänestyksessä.

Kansanäänestyksen tietoturvallisuusvaatimukset ovat löyhemmät kuin vaalien. Koska kuitenkin työryhmän keskustelut usein kääntyivät käsittelemään vaaleja, käsitellään dokumentissa myös vaalien tietoturvakysymyksiä. Huomattakoon, että tietoturvaa ei voi lisätä järjestelmään jälkikäteen kustannustehokkaasti. Vaikka on teoriassa mahdollista rakentaa ensin kansanäänestyksiin sopiva, vähemmän tietoturvallinen järjestelmä, sen laajentaminen myöhemmin vaaleihin sopivaksi maksaa olennaisesti saman verran kuin vaalijärjestelmä erikseen hankittuna. Toisin päin tehtävä on helpompi: vaalijärjestelmästä saa helposti kansanäänestysjärjestelmän, joskin järjestelmän hinta on silloin suurempi kuin pelkän vaalijärjestelmän hinta.

Kansanäänestyksen kustannusten ja hyötyjen suhde on olennainen päätettäessä toteutetaanko järjestelmä vai ei. Kustannusten ja hyötyjen arvioinnista on oma, erillinen kappaleensa.

Valtio voi joko toteuttaa järjestelmän valitsemillaan alihankkijoilla tai ostaa valmiin järjestelmän markkinoilta. Jotta valtio voisi päättää kumpi lähestymistapa on parempi, on ensin selvitettävä järjestelmän rajapinnat, millaisia järjestelmiä markkinoilla on, miten järjestelmä kannattaisi kilpailuttaa tai toteuttaa. Kaikista näistä on oma kappaleensa.

Lopuksi esitellään suunnitelman nettiäänestyksen toteutukselle ja käyttöönotolle. Suunnittelema rajoittuu vain kansanäänestyksen toteuttavaan järjestelmään.

Vaalijärjestelmän toteutusta ja käyttöönottoa kuvaillaan vain lyhyesti.

Järjestelmän toiminnallisuus

Nettiäänestysjärjestelmän tehtävänä on mahdollistaa äänestäminen neuvoa-antavissa kunnallisissa kansanäänestyksissä internetissä äänestäjän omaa päätelaitetta käyttäen. Tämän mahdollisuuden toivotaan lisäävän äänestysinnokkuutta ja lisäävän näin kansalaisten osallistumista päätöksentekoon.

Kansanäänestyksessä vaiheet ovat kirjeäänestys ja äänestyspäivä. Nettiäänestys voisi olla käytössä kirjeäänestyksen kanssa samaan aikana tai kirjeäänestyksen jälkeen tai myös äänestyspäivänä tai koko kansanäänestyksen ajan. Järjestelmän toiminnallisuus olisi erilainen riippuen järjestelmän käyttövaiheista.

Huomattakoon, että alla oleva keskustelu on vain pohdintaa. Päätös eri vaiheissa käytössä olevista äänestystavoista ja äänten korvautuvuudesta on luonteeltaan ennen kaikkea oikeudellinen[2]. Yleisenä periaatteena on oltava, että viranomaisen luona ja valvonnassa paperista äänestyslippua käyttäen tapahtuva ennakkoäänestys tai vaali-/äänestyspäivän äänestys luotettavampana korvaa aina nettiäänen.

1. Mikäli nettiäänestys tapahtuu ennen kirjeäänestystä, olisi luontevaa, että kirjeääni myöhemmin annettuna korvaisi aiemman tai aiemmat nettiäänet. Järjestelmä on rakennettava niin, että kunkin äänestäjän nettiääni on tunnistettavissa ja poistettavissa kirjeäänestyksen loppumisen jälkeen.
2. Mikäli nettiäänestys tapahtuu samaan aikaan kirjeäänestyksen kanssa, on päätettävä kumpi ääni on ratkaiseva. Tämä päätös ei voi perustua äänestämisajankohtaan, koska sen tarkka määrittäminen on hankalaa ja epävarmaa. Tämä on päätettävä lainsäädännössä. Päätös vaikuttaa järjestelmän toteuttamiseen ja toteuttamisen kustannuksiin.

[2] ks. Viron korkeimman oikeuden 1 päivänä syyskuuta antaman perustuslaillisen tuomion 3-4-1-13-05 perustelut

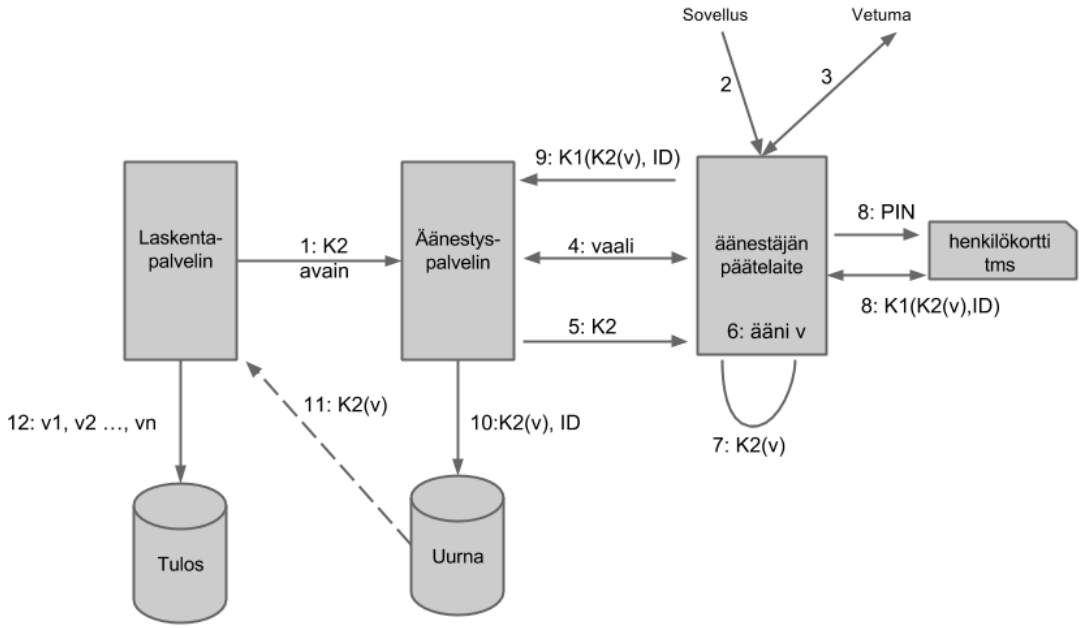
3. Mikäli nettiäänestys on käytössä myös varsinaisena kansanäänestyspäivänä, on myös luontevaa, että paperilla annettu ääni korvaa nettiäänen. Tämä johtuu siitä, että paperilla äänestyspaikassa annetun äänen väärentäminen (äänestäjän painostaminen tms) on vaikeampaa kuin nettiäänestyksessä.

Huomattakoon, että mikäli nettiäänestys on käytössä myös äänestyspäivänä, nettiäänestyksessä mahdollisesti tapahtuvia tietoturvaongelmia tai teknisiä epäselvyyksiä ei voi korvata mitätöimällä nettiäänestystä ja määräämällä vain äänestyspaikassa annettuja ääniä päteviksi. Tämä vähentää merkittävästi järjestelmän luotettavuutta ja mahdollisuutta toipua virheistä ja ulkopuolisten tahojen yrityksistä murtaa järjestelmän tietoturvallisuus. Tästä syystä ei suositella nettiäänestyksen käyttämistä äänestyspäivänä. Vastaava varovainen käytäntö on myös Virossa vaaleissa käytettävässä järjestelmässä.

Yhteenvetona todetaan, että todennäköisin vaihtoehto on kirjeäänestyksen korvaaminen nettiäänestyksellä, koska ainoastaan siten nettiäänestyksen käyttöönotto voi vähentää kustannuksia. Kustannukset syntyvät pääosin kirjeäänistä ja niiden käsittelystä.

Vastaava pätee myös vaaleihin. Tässä selvityksessä ei käsitellä vaaleihin mahdollisesti liittyviä seikkoja tähän asiaan liittyen tämän tarkemmin.

Kansanäänestyksen toteuttavan äänestysjärjestelmän keskeiset toiminnallisuudet ovat seuraavat.



Kuva 1: havainnekuva nettiäänestysjärjestelmästä

Järjestelmässä on seuraavat komponentit

- Äänestäjän sähköinen tunnistusväline, mobiilivarmenne tai vastaava
- Äänestäjän päätelaite
- Äänestyssovellus
- VETUMA
- Äänestyspalvelin
- Uurnatietokanta
- Laskentapalvelin
- Tulostietokanta

Järjestelmä toimii seuraavasti.

1: Laskentapalvelin lähettää keskusvaalilautakunnan julkisen avaimen K2 äänestyspalvelimelle. Keskusvaalilautakunta on luonut avaimen äänestystä perustaessaan.

2: Äänestäjä lataa äänestyssovelluksen päätelaitteelleen. Sovellus voi tulla äänestyspalvelimelta tai jostain muualta. Sovellus voi olla joko päätelaitteelle käännetty

natiivisovellus tai verkkosivulla oleva javascript-sovellus. Javascript on helpommin ja halvimmalla toteutettavissa oleva vaihtoehto.

3: Äänestäjä käyttää jotakin VETUMAn tarjoamaa vahvaa tunnistautumismenetelmää. Päätelaite saa tietoonsa äänestäjän identiteetin ID.

4: Äänestäjän päätelaite kysyy äänestyspalvelimelta kansanäänestykseen liittyvät tiedot (äänestysalueen, vaihtoehdot, jne) antamalla palvelimelle äänestäjän identiteetin ID. Nämä tiedot keskusvaalilautakunta on syöttänyt äänestyspalvelimelle ennen kansanäänestyksen alkamista. Tiedot voivat olla peräisin esimerkiksi väestötietojärjestelmästä tai vaalitietojärjestelmästä.

5: Äänestyspalvelin antaa äänestäjän päätelaitteelle keskusvaalilautakunnan julkisen avaimen K2.

6: Äänestäjä äänestää eli antaa äänen v päätelaitteensa äänestyssovellusta käyttäen.

7: Äänestäjän päätelaite salaa äänen avaimella K2. Tuloksena on K2(v)

8. Päätelaite allekirjoittaa äänen V ja identiteetin äänestäjän yksityisellä avaimella K1. Tuloksena on K1(K2(v), ID). Avain K1 on luotu äänestäjän käyttämän allekirjoituslaitteen alustamisen yhteydessä. Allekirjoituslaite voi olla esimerkiksi HST-kortti tai mobiilivarmenne. Tarkalleen ottaen allekirjoituslaite allekirjoittaa avainta K1 käyttäen, eikä avain K1 koskaan liiku allekirjoituslaitteen ulkopuolelle.

9: Äänestäjän päätelaite lähettää kohdan 8 tuloksen äänestyspalvelimelle.

10: Äänestyspalvelin tunnistaa äänestäjän avainta K1 vastaavaa julkista avainta käyttäen, varmistaa avaimen K1 ja identiteetin ID kuuluvan samalle henkilölle ja tallettaa parin (K2(v), ID) uurnatietokantaan. Nämä parit ovat uurnassa aikajärjestyksessä, jotta uusin voi aina korvata aiemmat äänet.

11: Äänestyksen loputtua äänestyspalvelin 1 lähettää kunkin äänestäjän salatut äänet laskentapalvelimelle 2. Tämä voi tapahtua myös jotain fyysistä mediaa käyttäen tietoturvan parantamiseksi.

12: Palvelin 2 purkaa äänien salaukset omalla salaisella avaimellaan ja tallettaa äänet tietokantaansa.

Huomattakoon, että järjestelmä voidaan toteuttaa myös ilman avaimen K1 käyttöä, mutta tällöin järjestelmän tietoturva on merkittävästi huonompi. Tällöin näet äänestäjän päätelaitteen ja äänestyspalvelimen välillä oleva vihamielinen taho voi väärentää äänet. Kansanäänestyksen tapauksessa tämä kuitenkin voi olla tarpeeksi hyvä ratkaisu.

Vaaleissa avaimen K1 käyttäminen on ehdottoman välttämätöntä vaalien eheyden varmistamiseksi. Näin ollen esimerkiksi nykyisen Tupas-tunnistuksen kaltainen tunnistautuminen ei ole riittävä vaalien tietoturvallisuuden takaamiseksi.

Huomattakoon, että tässä mallissa on luotettava äänestäjän päätelaitteella olevaan sovellukseen. Mikäli hyökkääjä[3] pääsee sopivasti vaihtamaan sovelluksen, hän voi väärentää äänestäjän äänen. Tämän hyökkäyksen mahdollisuuden poistaminen on erittäin vaikeata. Kansanäänestyksen tapauksessa se ei kuitenkaan ole tarpeellista, koska tässä esitetty järjestelmä on vähintäänkin yhtä turvallinen ja luotettava kuin nykyinen kirjeäänestys.

Järjestelmävaatimukset

Tämä kappale esittelee nettiäänestysjärjestelmälle yleisesti esitettäviä vaatimuksia. Nämä vaatimukset ovat suurelta osin peräisin nykyisistä kansanäänestyksistä ja vaaleista. On luontevaa, että nettiäänestystä koskevat samat vaatimukset kuin perinteisempää lippuäänestystä. Lisäksi on olemassa joitakin nettiäänestykseen liittyviä erityisiä vaatimuksia. Nämä ovat tulleet esiin nettiäänestystyöryhmän työn aikana.

Huomattakoon, että tietoturvallisuuteen liittyviä vaatimuksia ja niihin liittyviä asioita käsitellään laajemmin luvussa tietoturvallisuus alempana.

V1: Äänestäjän henkilöllisyys ja äänioikeus on todettava luotettavasti

Äänestysjärjestelmän on pystyttävä varmistamaan, että vain kussakin äänestyksessä äänioikeutetut voivat äänestää.

Kuvan 1 mukainen järjestelmä täyttää tämän vaatimuksen. VETUMA-järjestelmä on luotettava henkilöllisyyden tunnistamisen väline. Järjestelmä myös pystyy varmentamaan äänioikeuden: palvelin 1 antaa äänestäjän päätelaitteelle tiedot vain niistä äänestyksistä, joissa äänestäjällä on äänioikeus.

Vaalien suhteen on huomattava, että avaimen K1 käyttäminen on mahdollista vain mikäli käytössä on jokin allekirjoitustoiminnallisuuden sisältävä tunnistautumisjärjestelmä.

V2: Kukin äänioikeutettu voi antaa vain yhden äänen

[3] Hyökkääjä on jokin ulkopuolinen taho, joka pyrkii järjestelmällisesti vaikuttamaan äänestyksen tulokseen.

Suomessa käytössä olevissa vaaleissa ja äänestyksissä kullakin äänestäjällä on vain yksi ääni käytettävissään. Järjestelmän on huolehdittava, ettei kukaan pääse äänestämään useaan kertaan.

Kuvan 1 mukainen järjestelmä täyttää tämän vaatimuksen. Uurnasta siirretään palvelimelle 2 vain kunkin äänestäjän viimeksi antama ääni. Äänestyspäivänä mahdollisesti annettavien paperiäänten ja nettiäänten välinen valinta ei ole kuvan 1 mukaisen järjestelmän tehtävä vaan tapahtuu jossakin muussa järjestelmässä. Luonteva vaihtoehto on vaalitietojärjestelmä[4].

Kuva 1 mukaisessa järjestelmässä on myös mahdollista rajoittaa kunkin äänestäjän äänien määrä yhteen - eli niin, ettei äänestäjä voi korvata antamaansa nettiääntä uudella nettiäänellä.

Vaalien suhteen on huomattava, että ilman avainta K1 - ja myös sen kanssa - on hyvin vaikeaa varmistua siitä, että äänestäjä on itse antanut viimeisenä uurnaan saapuneen äänen. Äänen on näet voinut antaa myös päätelaitteessa olevan ohjelman omalla ohjelmallaan korvannut hyökkääjä.

V3: Äänestyssalaisuus on turvattava

Nettiäänestyksissä äänestyssalaisuus on yleisesti pyritty turvaamaan mahdollisuudella äänestää useasti. Kuvan 1 mukainen järjestelmä täyttää tämän vaatimuksen. Tämä edellyttää, että äänestyspalvelimen operaattorit eivät voi mitenkään saada tietoonsa laskentapalvelimen yksityistä avainta ja että avainta K2 käyttävä salausmenetelmä on riittävän vahva.

Lisäturvallisuutta on mahdollista järjestää sopimalla, että äänestyspäivänä annettava lippuääni on ratkaiseva. Tällöin koko kansanäänestysjärjestelmä on tämän vaatimuksen suhteen yhtä turvallinen kuin nykyisin käytössä ole paperiäänestysjärjestelmä.

Vaalien suhteen tilanne on sama, koskien tietenkin vaalisalaisuutta.

V4: Annettua ääntä ei kukaan saa päästä muuttamaan

Kuvassa 1 esitetty järjestelmä täyttää tämän vaatimuksen, mikäli äänestystä operoivat henkilöt ovat luotettavia ja palvelinten tietoturva on moitteeton. Mikäli hyökkääjä pääsee salaisesti käsiksi molempiin palvelimiin ja salausavaimiin, hän voi muuttaa ääniä niin, ettei sitä välttämättä ole mahdollista huomata. Kansanäänestyksen suhteen tämä ei ole suuri ongelma, koska äänestys on vain neuvoa-antava. Ainoa mahdollinen tapa varmistua äänen muuttumattomuudesta on järjestelmän kattava auditointi, joka lisää järjestelmää kohti tunnettua

[4] Mahdollinen on vaalitietojärjestelmän ohella nykyisin kaikissa kunnallisissa kansanäänestyksissä noudatettava menettely, jossa kirjeäänestykset (oikeastaan äänioikeuden lopullinen käyttö kirje-/ennakkoäänestyksessä) merkitään manuaalisesti äänestysluetteloihin. Tämä luonnollisesti vaatii järjestelmältä tuen tällaiseen toimintatapaan.

luottamusta. Tilanne on nykyisinkin aivan sama: vain luottamus on muuttumattomuuden takeena.

Huomattakoon, että on hyvin vaikeata huomata hyökkääjän muuttaneen ääniä. Taitava hyökkääjä osaa peittää jälkensä. Ainoa keino huomata äänten muuttuminen lienee nettiäänestyksen tuloksen vertaaminen esimerkiksi lippuäänestyksen tulokseen, gallup-tutkimuksiin tai muuhun. Tämäkään ei ole kovin helppoa, koska on aivan mahdollista, että nettiäänestyksen äänten jakauma on eri kuin gallupin ennustama tai äänestyspäivänä annettujen äänten.

V5: Äänestäjän tulee voida varmistua siitä, että hänen äänensä on kirjautunut äänestysjärjestelmään hänen tarkoittamallaan tavalla

Tavallisessa lippuäänestyksessä äänestäjä pudottaa äänensä uurnaan ja luottaa sen kirjautumiseen. Nettiäänestyksessä äänen kirjautuminen uurnaan vastaavaan tietojärjestelmään on paljon abstraktimpi tapahtuma. Tästä syystä äänestäjän on jollakin tavalla saatava järjestelmästä kuittaus äänen perillemenosta muuttumattomana.

Kuvan 1 mukainen järjestelmä ei täytä tätä vaatimusta. Järjestelmään on kuitenkin mahdollista liittää esimerkiksi Virossa käytettävissä olevan kaltainen kanava, jolla äänestäjä pystyy pyytämään palvelimilta tiedon uurnaan menneestä äänestään. Viron järjestelmässä tämä tapahtuu niin, että äänestäjä äänestää tietokoneellaan ja ottaa mobiililaitteellaan kuvan äänestyssovelluksen luomasta QR-koodista. Äänestäjä lähettää koodin äänestyspalvelimelle, joka vastaa tiettyä protokollaa käyttäen. Äänestäjän mobiilisovellus pystyy päättelemään mitä äänestäjä on äänestänyt ja näyttämään sen äänestäjälle.

Tämä vaatimus ei välttämättä ole olennainen kansanäänestyksistä, koska niissä käytettävä kirjeäänestys ei ole 100% luotettava. Äänestäjä ei voi kirjeäänestyksessäkään olla varma äänensä kirjautumisesta järjestelmään. Tämä johtuu siitä, että posti toimittaa perille alle 100% kirjeistä.

Vaaleissa tämän vaatimuksen on ehdottomasti täytyttävä. Vaatimuksen täyttäminen on hankalaa, koska vaaliviranomaisilla ei ole mitään helposti toteutettavaa keinoa varmistua, että äänestäjien päätelaitteilla käyttämä ohjelmisto ei ole taitavasti väärennetty.

Huomattakoon, että esimerkiksi Norjassa käytössä olleessa nettiäänestysjärjestelmässä on pyritty varmistamaan vaatimusten V4 ja V5 toteutuminen monimutkaisin teknisin menettelyin. Näissä menettelyissä järjestelmä palauttaa äänestäjälle eri tavoin tiedon äänestyspalvelimelle kirjautuneesta äänestä. Tämä lisää järjestelmän luotettavuutta. Menetelmät tosin ovat niin

monimutkaisia, että niiden ymmärtäminen on mahdollista vain hyvän tietoteknisen koulutuksen omaaville. Muiden on vain luotettava järjestelmään.

V6: Äänestäjän on voitava varmistaa, että annettu ääni on oikein laskettu mukaan äänestyksen tuloksiin

Tavallisessa paperiäänestyksessä tätä vaatimusta ei ole vaan äänestäjän on yksinkertaisesti luotettava vaalilautakuntien rehellisyyteen ja vaalilautakuntien jäsenten keskinäiseen valvontaan.

Kuvan 1 mukaisessa järjestelmässä tätä vaatimusta ei ole mahdollista täyttää äänestyssalaisuutta vaarantamatta. Vaatimuksen voi toteuttaa, mikäli äänet lasketaan äänestyspalvelimella, mutta tällöin joudutaan vaarantamaan äänestyssalaisuusvaatimus. Tämä johtuu siitä, että laskentapalvelimelle ei ole tietoa äänen antajan identiteetistä.

V7: Äänestyksen tulos on voitava luotettavasti todentaa ja tarkastaa jälkikäteen

Kuvan 1 mukaisessa järjestelmässä tulostietokanta voidaan rakentaa siten, että sen muuttaminen äänestyksen jälkeen on mahdotonta. Tällöin äänet on mahdollista laskea uudestaan milloin vain. Äänten laskeminen usealla toisistaan riippumattomalla ohjelmistolla on omiaan lisäämään luottamusta laskennan oikeellisuuteen. Tämä on teknisesti aivan mahdollista.

On huomattava, että äänestyksen tulos koostuu annettujen äänten lisäksi äänestyksen aikana pidettävistä lokeista. Ne on myös säilytettävä muuttumattomina. Lokien mukaan annettujen äänien (eli äänestäneiden määrän) ja uurnassa olevien äänien määrän on täsmättävä.

V8: Nettiäänestämisen tulee olla mahdollista äänestäjien yleisesti käyttämillä laitteilla

Kuvan 1 mukainen javascriptillä toteutettu nettiäänestysjärjestelmä toimii kaikilla moderneilla päätelaitteilla. Tämä luonnollisesti estää vanhempien päätelaitteiden käytön.

V9: Äänestysjärjestelmä, jota saadaan käyttää kaikissa Suomessa järjestettävissä vaaleissa ja kunnallisissa sekä valtiollisissa kansanäänestyksissä, tulee kokonaan valtion omistukseen ja hallintaan

Kuvan 1 mukainen järjestelmä on helppoa pitää valtion omistuksessa ja hallinnassa. Valtiolla on jo nyt olemassa menettelyt teettämiensä, ostamiensa ja käyttämiensä ohjelmistojen omistuksen ja hallinnan hallintaan. Menettelyt ovat varmasti riittävät nettiäänestysjärjestelmänkin kohdalla.

V10: Äänestysjärjestelmän, mukaan luettuna lähdekoodi ja järjestelmän tekniset kuvaukset, tulee olla tutustumista varten kokonaan julkinen kansalaisille, järjestöille, asiantuntijoille ja vaalitarkkailijoille.

Ei ole nähtävissä mitään syytä, miksi kuvan 1 mukaisen järjestelmän toteuttava toimittaja ei suostuisi vastaan avaamaan lähdekoodiaan vaikkapa github-palveluun. Tämä on olennaisen tärkeätä järjestelmä luotettavuuden lisäämiseksi. Tämä vaatimus ei varsinaisesti koske järjestelmää vaan järjestelmän toteutuksesta tehtäviä sopimuksia.

V11: Äänestysjärjestelmän on oltava esteetön

Järjestelmän käyttöliittymän on oltava näkövammaisten ja muiden eri tavoin esteellisten käytettävissä. Kansanäänestyksissä on vain muutamia vaihtoehtoja, joten ne on helppoa esittää millä tahansa päätelaitteella niin, että esteettömyys ei vaarannu.

Vaaleissa ehdokkaita voi olla satoja. Satojen ehdokkaiden esittäminen pienellä päätelaitteella on käytettävyysongelma. Ongelma on kuitenkin huolellisella suunnittelulla ratkaistavissa.

V12: Äänestysjärjestelmän on oltava puolueeton

Tämä käytettävyysvaatimus vaikea toteuttaa erityisesti pieniä mobiililaitteita käytettäessä. Pienelle ruudulle mahtuu vain muutama ehdokas kerrallaan. On varmistauduttava, etteivät ruudulle ensimmäisenä tulevat ehdokkaat saa tästä etua itselleen. Tämä voidaan toteuttaa esimerkiksi esittämällä ehdokkaat satunnaisessa järjestyksessä.

V13a: Yhteensopivuus VAT:n kanssa

Äänestysjärjestelmän on oltava yhteensopiva nykyisen vaalitietojärjestelmän (VAT). VAT tarjoaa nettiäänestysjärjestelmälle tiedot äänestäjistä, vaalipiireistä, äänestysalueista ja muista äänestyksessä tarvittavista tiedoista. Nettiäänestysjärjestelmä tarjoaa VAT:lle tiedot äänestyksen tuloksista, jotka VAT sitten jakelee eteenpäin.

V13b: Toimivuus ilman VAT:ää

Äänestysjärjestelmän on (vaatimuksen V13a kanssa vaihtoehtoisesti) tarjottava rajapinnat äänestyksen järjestämiseen tarvittavien tietojen syöttämiseen ja/tai poimimiseen muista järjestelmistä. Tämä vaatimus on tarpeen siksi, että joissakin tilanteissa VAT:n käyttäminen ei mahdollisesti ole teknisesti tai taloudellisesti tarkoituksenmukaista.

Tietoturvallisuus

Tietoturvallisuusvaatimukset tulisi aina asettaa toiminnan ja järjestelmän riskianalyysin kautta. Koska järjestelmää ei vielä ole, työssä analysoitiin vaali- ja äänestysprosessia tapauksessa, jossa nettiäänestys olisi käytössä jossain roolissa. Näillä lähtötiedoilla analyysi oli varsin kevyt, eikä sitä voida pitää riittävänä riskianalyysinä varsinaista järjestelmäkehitystä varten. Sen sijaan

sillä saatiin esille joitakin järjestelmän kustannuksiin olennaisesti liittyviä uhkia. Varsinainen riskianalyysi voidaan tehdä, kun järjestelmän toiminnallisuus on täysin päätetty.

Tietoturvallisuustarpeiden analyysiä monimutkaisti kolme tosiasiaa, jotka aiheuttivat ristiriitaisia vaatimuksia. Ensinnäkin ei ollut päätöksiä, missä roolissa nettipohjainen järjestelmä olisi osana vaali- tai äänestysprosessia ja mitkä olisivat toiminnallisuuden rajat. Missä mitassa sähköinen menetelmä olisi käytössä muiden perinteisten tapojen rinnalla? Olisiko se käytössä pelkästään ennakkoäänestyksessä, vai myös vaalipäivänä? Halutaanko mahdollisuutta uudelleenäänestykseen, jolloin uusi ääni korvaisi vanhan? Kaikki nämä kysymykset vaikuttavat järjestelmän toimintaan, arkkitehtuuriin ja sitä myöten tietoturvallisuusvaatimuksiin.

Toiseksi, valtiollisten vaalien uhkamalli on hyvin erilainen kuin kunnallisen neuvoa-antavan kansanäänestyksen. Valtiollisiin vaaleihin voivat haluta vaikuttaa paitsi Suomen sisäiset ryhmät, myös mahdolliset ulkopuoliset tahot. Maailmalta löytyy esimerkkejä, joissa ulkopuolisilla valtiollisilla tahoilla on ollut suuret resurssit käytössään niiden hyökätessä haittaohjelmalla kohdemaan infrastruktuuria vastaan. Sähköisiä vaaleja vastaan on jo hyökätty tietoteknisin keinoin[5], tosin kyseessä ei tällöin ollut valtiollinen taho. Tästä voidaan kuitenkin päätellä, että valtiollinen hyökkäys vaaleihin ei ole täysin mahdoton uhkaskenaario. Hyökkäyksen ei edes tarvitse onnistua kovin hyvin, jotta se loisi epäluottamusta kansallisen vaalituloksen oikeellisuuteen ihmisten mielissä. Kansanäänestys taas kohdistuu kunnalliseen päätöksentekoon ja sen tulokset antavat tietoa päätöksenteon pohjaksi. Jos on epäilystä tai todisteita, että sähköisen kansanäänestyksen tulosta on manipuloitu, sen tulokset voidaan jättää huomiotta. Tällaisen ongelman esiin tuleminen voi olla paikallisesti merkittävä epäluottamusta aiheuttava tekijä, mutta koko yhteiskunnan mittakaavassa pieni. Tämän tarkastelun perusteella ongelmat kansanäänestyksen tietoturvallisuudessa aiheuttavat lievempiä seurauksia kuin vastaavat ongelmat valtakunnallisissa vaaleissa. Kansanäänestykseen tarvittavan järjestelmän tietoturvallisuuspiirteet voisivat siis olla kevyempiä kuin valtiollisen vaalijärjestelmän.

Kolmanneksi, edellä esitetystä huolimatta tietoturvayhteisön konsensus on, että järjestelmän tietoturvavaatimuksia luotaessa on aina lähdettävä tietoturvaltaan vaativimman käyttötapauksen mukaan. Jos järjestelmä on rakennettu esimerkiksi ST[6] IV aineiston käsittelyä varten, sen nostaminen jälkikäteen ST III tai II -materiaalin käsittelyyn kelpaavaksi ei välttämättä onnistu, tai jos onnistuu niin kustannukset voivat olla suuret. Syynä tähän on se, että alussa asetetut tietoturvallisuusvaatimukset määrittävät arkkitehtuuri-, komponentti- ja tuotevalintoja (esim.

[5] Itävalta, opiskelijavaalit, 2009

[6] ST-luokitus ei täysin sovellu nettiäänestyksen tietoturvallisuuden määrittämiseen, mutta sitä on kuitenkin käytetty esiselvityksessä pohjana, koska muutakaan paremmin soveltuvaa luokitusta ei ole tarjolla.

tietokannan salausmahdollisuus, ohjelmiston eri kerroksilla tarvittavat tietoturvapiirteet, tarvittavat tietoliikennejärjestelyt). Näiden alussa tehtyjen valintojen muuttaminen jälkikäteen uusia tietoturvavaatimuksia vastaaviksi on käytännössä yhtä kallista kuin uuden järjestelmän rakentaminen. Järjestelmää hankittaessa on siis jo aikaisessa vaiheessa tehtävä päätös, halutaanko järjestelmää käyttää pelkästään kunnallisiin kansanäänestyksiin vai myös valtiollisiin vaaleihin. Tätä päätöstä ei voi tehdä jälkikäteen jos kustannustehokkuudesta halutaan pitää kiinni. Päätöksen voi lykätä, jos kustannustehokkuus ei ole huomioon otettava näkökohta.

Näiden vuoksi työpajassa löydetyt uhat eivät ole aivan yhteismitallisia. Osa niistä voi toteutua vain tietyissä järjestelmän käyttötavoissa, tietyissä tilanteissa tai tietyillä arkkitehtuureilla. Merkittävimmät löydetyt uhat olivat:

- Toimittajan kyvyttömyys toimittaa tietoturvallinen järjestelmä. Tämä voidaan ratkaista tietoturva-auditoinneilla sekä avoimen lähdekoodin mallilla, mahdollisesti myös hajauttamalla kehitystä usean toimittajan kesken.
- Päätelaitteen ja sen ohjelmiston turvallisuus.
- Palvelunestohyökkäykset joko itse nettiäänestysjärjestelmään tai johonkin kolmannen osapuolen hallitsemaan järjestelmään, jonka toiminnasta sähköinen äänestys on riippuvainen (esim. tunnistuspalvelut).
- Tietoturvallisuutta vaarantavat virheet vaalijärjestelmään liittyvissä alustus- ja ylläpitotoimissa. Esimerkiksi Viron vuoden 2013 vaalien toimista on löydetty useita tähän liittyviä ongelmia[7]. Tämän vuoksi sähköisen äänestyksen järjestelmän käyttö- ja ylläpitoprosessien suunnitteluun ja valvontaan on panostettava merkittävästi.
- Puutteet järjestelmän valvonnassa ja kyvyssä reagoida vaalijärjestelmään kohdistuviin tietoturvahyökkäyksiin. Tämä voidaan ratkaista panostamalla operointiin riittävillä resursseilla ja rakentamalla järjestelmään riittävät lokitus- ja valvontamekanismit.

Tietoturvallisuuden ja varautumisen taso

Tietoturvallisuustyöpajassa käytiin läpi haluttu tietoturvallisuuden ja varautumisen taso valtionhallinnon kriteerien mukaan. Vaikka tietoturvallisuusasetuksen täyttäminen ei olekaan pakollista kansanäänestystä järjestävien kuntien järjestelmissä, tämän järjestelmän omistaja on oikeusministeriö, joka tarjoaa tätä palveluna myös kunnille (ks. vaatimus V9 edellä). Näin ollen

[7] Springall et al, “Security Analysis of the Estonian Internet Voting System”, ACM CCS’14.

tietoturvallisuusasetus[8] ja valtionhallinnon tietoturvallisuustasot ovat olennaisia huomioon otettavia vaatimuksia tämän järjestelmän kohdalla.

Alussa pohdittiin järjestelmän yhteiskunnallista merkittävyyttä, ja todettiin että *vaaliprosessi* on yhteiskunnallisesti elintärkeä. Vaaliprosessissa on useita eri osa-alueita ja toimintoja, joista sähköinen äänestys on vain yksi sivujuonne.

Tärkeintä vaaleissa ja kansanäänestyksissä on tapahtuman eheys. Tämä tarkoittaa että järjestelmän tulee kaikissa tilanteissa pitää huoli siitä, että annettu ääni ei muutu matkalla ja lasketaan hyväksi vain äänestäjän valitsemalle vaihtoehdolle (ks vaatimus V4 edellä).

Tietoturvallisuusasetus lähtee siitä, että viranomaisen asiakirjat tulee luokitella. Tämän seurauksena tietojärjestelmiin, joissa kyseistä luokiteltua asiakirjaa käsitellään, tulee toteuttaa luokitusta vastaavan tietoturvallisuustason vaatimukset mm. salassapitoon ja käyttörajoituksiin liittyen. Tietosisällön luokittelu on siis olennainen osa järjestelmän vaatimusmäärittelyä, koska se määrittelee käytännön tietoturvavaatimuksia. Jos järjestelmässä käsitellään monen eri suojaustason aineistoja, järjestelmän arkkitehtuuri voidaan toki suunnitella niin, että vain välttämättömin mutta silti riittävä osa järjestelmästä on kovimmalla tietoturvallisuustasolla.

Valtakunnallista vaalijärjestelmää arvioitaessa todettiin, että vaalisalaisuuden vuoksi (ks vaatimus V3) osa vaaleissa käytettävän järjestelmän tietosisältöä on suojaustasoa III. Jos järjestelmässä säilytetään ääniä niin, että äänestäjän identiteetti on yhdistettävissä annettuun ääneen, kasautumisvaikutuksen vuoksi tämä tietovarasto voi olla jopa suojaustasoa II. Tämän ST II -luokituksen toteutus aiheuttaisi merkittäviä hankaluuksia järjestelmän tekniselle arkkitehtuurille, sillä suojaustason II toteuttavat komponentit eivät saa olla yhteydessä julkiseen Internetiin. Vaikka em. tietovarastossa ääni olisikin salattu ja siitä ei salausta purkamatta voisi päätellä, ketä äänen antaja on äänestänyt, täytyy muistaa että vaalisalaisuuden ja sitä myöten salauksen tulee olla murtumaton siihen asti kunnes äänet hävitetään.

Kunnallisen kansanäänestyksen osalta lainsäädännössä on edellä mainittua vaalisalaisuutta vastaava äänestyssalaisuus[9]. Tämän vuoksi voidaan ajatella, että suojaustaso olisi kunnallisen kansanäänestyksen äänille vaalia vastaava ST III. Keskustelussa on kuitenkin esitetty myös näkemyksiä, että sähköisen kansanäänestyksen tietosisältö kuuluisi lievemmälle suojaustasolle IV kahdesta syystä. Ensinnäkin tietosuoja-asetuksen 9§ mainittu suojaustasojen ero perustuu annetun äänen paljastumisen seurauksia kuvailevien fraasien "voi aiheuttaa haittaa" (ST IV) ja "voi aiheuttaa vahinkoa" (ST III) tulkintaan, mikä voi olla erilainen vaalin ja kansanäänestyksen

[8] Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010

[9] Laki neuvoa-antavissa kunnallisissa kansanäänestyksissä noudatettavasta menettelystä, 16§

välillä. Toiseksi, nykyisessä kansanäänestyksessä paperisia äänestyslippuja ei käsitellä suojaustason III mukaisesti. Siitä, miten asiakirjoja perinteisesti käsitellään ei kuitenkaan voi täysin varmasti päätellä siitä, miten asioiden tulisi uuden lainsäädännön valossa olla. Siksi luokittelu tulee ratkaista erikseen. Tämä päätös tulee vaikuttamaan merkittävästi sähköisen kansanäänestyksen järjestelmävaatimuksiin. Tässä työssä myös äänten kasautumisvaikutus on otettava huomioon kuten vaalitapauksessa yllä.
Järjestelmän saatavuusprofiili on normaalista tietojärjestelmästä hyvin poikkeava. *Valtiollista vaalijärjestelmää käytetään nykyisellä yhteiskuntamallilla keskimäärin kerran vuodessa (0-2 kpl/vuosi), jolloin järjestelmä on käytössä joitakin kuukausia kerrallaan vaalia kohti.* Kunnallisia kansanäänestyksiä sen sijaan voisi olla vuodessa useita jos useat kunnat ottaisivat tällaisen sähköisen välineen aktiiviseen käyttöön. Kuitenkin tässäkin tapauksessa järjestelmä olisi mahdollisesti käytössä vain osan aikaa vuodesta. Järjestelmälle ei siis tarvita samaa saatavuuden palvelutasoa koko vuoden ajan.

Kuitenkin äänestysaikana järjestelmän saatavuus on erittäin tärkeä. Tällöin 24/7-tyyppinen palvelutaso ja nopea häiriönselvityksen vasteaika erityisesti teknisten ongelmien varalta on olennaista. Saatavuus tulee entistä kriittisemmäksi jos järjestelmä on käytössä vaalipäivänä. Valtorin arviointipohjan tärkeimmässä saatavuuskategoriassa on häiriöille 2 tunnin ratkaisuaika ja JHS174:ssä 3h. Näinkin lyhyt häiriö aiheuttaisi ongelmia ihmisten äänestysmahdollisuuksille vaalipäivänä, jos häiriö ajoittuu äänestysajan loppuun, jolloin äänestäjä ei enää ehdi käyttää vaihtoehtoisia tapoja. Näin ollen em. valmiit kategoriat eivät käy vaalipäivänä käytettävälle järjestelmälle, vaan palvelutaso on sovittava räätälöidysti. Näin onkin jo tehty nykyisille vaalitietojärjestelmän komponenteille.

Kansanäänestyksiin sopivan järjestelmän tietoturvallisuuden taso riippuu tietosisällön luokituspäätöksestä ja siitä, halutaanko järjestelmän olevan käytössä myös vaali- eli äänestyspäivänä.

- Jos kansanäänestyksen äänien suojaustaso lasketaan tasolle IV, järjestelmän tietoturvallisuustaso on tasolla **korotettu.**
- Jos sähköisen järjestelmän ei tarvitse olla käytössä vaalipäivänä ja sallitaan enintään 7h toimintakatkot, ICT-varautumisen taso on **korotettu**.
- Jos sähköisen järjestelmän tulee olla käytössä vaalipäivänä, ICT-varautumisen tason tulee olla **korkea** ja häiriönselvityksen vasteaika tulee sopia kaikkien palveluntarjoajien kanssa erikseen riittävän korkealle tasolle.

*Valtiollisiin vaaleihin sopivan järjestelmän (äänien suojaustaso III) tietoturvallisuustaso sekä ICT-varautumisen taso on **korkea**.*

Lisävaatimukset tietoturvallisuuden osalta

Edellä esitetty ja työpajassa läpikäydyt uhat luovat ainakin seuraavat tietoturvallisuuteen liittyvät lisävaatimukset:

V14: Järjestelmän tulee mahdollistaa ST IV (*vaaleissa ST III*) tietoaineiston käsittely, toiminnallisista vaatimuksista riippuen mahdollisesti jopa ST III (*vaaleissa ST II*).

V15: Järjestelmän tietoturvatason tulee olla korotettu (*vaaleissa korkea*).

V16: Järjestelmän ICT-varautumisen tason tulee olla korkea.

V17: Jos järjestelmä on käytössä myös vaalipäivänä, saatavuuden tulee olla paremmalla tasolla kuin Valtorin tai JHS 174:n korkein kategoria.

V18: Sähköisen järjestelmän vaalikohtaiset prosessit (asennus, tietojen syöttö yms) ja avainten luontiin liittyvät seremoniat[10] on suunniteltava huolellisesti, niin että teknisten ja tietoturvallisuutta vaarantavien virheiden mahdollisuus minimoidaan.

V19: Sähköisen järjestelmän vaalikohtaiset prosessit ja avainten luontiin liittyvät seremoniat on toteutettava huolellisesti suunnitelman mukaan ja prosessin/seremonian eri vaiheiden suorittamisesta on jäätävä verifioitava todiste.

V20: Järjestelmän tulee pitää eri tason lokeja teknisestä toiminnastaan (mm. käyttöjärjestelmä-, tietoliikenne-, tietokanta- ja sovellustasot) kuitenkin niin, että niiden tietoja yhdistämällä ei voida rikkoa vaali- ja äänestyssalaisuutta.

V21: Järjestelmän prosessien, seremonioiden ja teknisen toiminnan tulee mahdollistaa ETYJin vaalitarkkailuohjeistuksen mukainen tarkkailu.

V22: Vaalien ja/tai äänestyksen aikana tulee olla riittäviä resursseja mahdollisten tietoturvahyökkäysten havaitsemiseen ja selvittämiseen reaaliajassa.

V23: Järjestelmää ylläpitävän tahon (tekninen palveluntarjoaja) ja äänestyksen/vaalin toimeenpanevien henkilöiden oikeudet ja roolien eriytys järjestelmissä tulee suunnitella ja toteuttaa huolella niin, että yksittäinen henkilö ei pääse estämään äänestystä/vaalia tai manipuloimaan tulosta.

[10] Seremonia on esim. varmenteiden avainten luonnissa käytetty määrämuotoinen operaatio, jonka suorittamiseen tarvitaan useampi henkilö, ja jolle valitaan puheenjohtaja.

Jäljelle jäävät uhat

Edellä kuvatut vaatimukset auttavat pienentämään joitakin havaittuja uhkia. Kuitenkin on uhkia, joita ei voida helposti ratkaista toiminnallisten vaatimusten vuoksi. Esimerkiksi seuraavat uhat ovat edelleen olemassa:

- Äänestyssalaisuus ja -eheys lepää tiukasti päätelaitteen turvallisuuden varassa. Päätelaitteisiin voi tulla erilaisia kohdistettuja haittaohjelmia, jotka estävät äänestyksen tai erehdyttävät äänestäjää antamaan äänensä väärälle henkilölle. Uhka on merkittävä tilanteessa, jossa äänilippua ei salata äänestäjän salaisella avaimella, vaan luotetaan pelkästään äänestäjän tunnistukseen (kuvan 1 tapaus, jossa ei ole avainta K1).
- Sähköisen äänestysjärjestelmän toimittaja ja tekijät ovat avainroolissa äänestyksen turvallisuuden ja tuloksen oikeellisuuden kannalta. Kehityksen hajauttamisella useaan organisaatioon, kolmansien osapuolten tekemillä testauksilla, auditoinneilla tai avoimen lähdekoodin mallilla voidaan tätä riskiä lieventää, mutta ei kokonaan poistaa.
- Järjestelmää ylläpitävän tahon teknisellä henkilöstöllä on suuret mahdollisuudet häiritä ja estää nettiäänestystä sen eri vaiheissa. Paperilla tapahtuvaan äänestykseen verrattuna tilanne on erilainen siinä mielessä, että palveluntarjoajan yksittäisillä henkilöillä on laajoja pääsyoikeuksia ja -valtuuksia järjestelmän kokonaisinfrastruktuuriin, eikä teknisen ylläpidon toiminnassa ole normaalisti samanlaista usean osapuolen valvontaa kuin esim. ääntenlaskennassa. Nykyiset tämän alueen riskienhallintamekanismit nojaavat sopimuksiin, jotka eivät kuitenkaan varsinaisesti estä tällaisia tapahtumia. Riskiä voidaan lieventää kehittämällä teknisen henkilökunnan valvontaa esim. teknisen valvontalautakunnan muodossa.
- Sähköinen äänestys on hyvin riippuvainen ulkopuolisista toimijoista (VETUMA ja pankkitunnistus, palvelu- ja tietoliikenneoperaattorit yms), joiden toimintahäiriöt tai joihin kohdistuvat kyberhyökkäykset voivat vaikuttaa sivutuotteena myös sähköiseen äänestykseen.
- Ei ole sovittu, miten sähköisessä järjestelmässä tapahtuu äänestyksen arkistointi ja mahdollinen vaalin/äänestyksen jälkikäteinen verifioitavuus. Pitkäaikainen arkistointi luo pitkäaikaisen riskin.

Jos sähköistä äänestystä halutaan käyttää, nämä jäännösriskit on käsiteltävä hyvän riskienhallintatavan mukaisesti. Ne on joko hyväksyttävä, kehitettävä lisäkontrolleita em. riskien pienentämiseksi hyväksyttävälle tasolle, tai todettava että sähköistä järjestelmää ei voida ottaa käyttöön.

Hyötyjä

Hyötyjä arvioidaan olettaen eri tahoilta saatujen tietojen perusteella[11] [12] [13], että kunnallisen kansanäänestyksen kokonaiskulut äänioikeutettua kohden eivät nouse yli normaalien kunnallisvaalien kulujen, jotka suurinpiirtein ovat yhtä vaalia kohden kokonaisuudessaan hiukan yli 5€/annettu ääni. Tästä kuntien osuus on noin 4€/annettu ääni. Viime aikoina suoritetuista kunnallisvaaleista voidaan huomata, että karkeasti ottaen 70-80% vaalien kuluista tulee kunnille lankeavista kuluista, loput ovat valtakunnallisia kuluja. Kuntien kuluja korvataan valtion puolelta oikeusministeriön suorittamilla korvauksilla valtiollisissa vaaleissa.

Jos nettiäänestysjärjestelmä pystyy vähentämään kunnissa tehtävää äänestyksen valvonta- ja laskentatyötä, tulisi yllä olevan perusteella järjestelmästä merkittävää hyötyä. Karkealla tasolla kunnissa tehtävä valvonta- ja laskentatyö muodostaa ⅔ äänestyksen kustannuksista kunnissa, mikäli oletamme kansanäänestykselle saman kustannusrakenteen kuin kunnallisvaaleille.

Taloudellinen tekijä ei ole tietenkään ainoa mahdollinen hyötytekijä nettiäänestysjärjestelmästä. Mahdollinen äänestäjien aktivoiminen äänestyksen helppouden kautta ja siten demokratian vahvistaminen yhteiskunnassa on myös varteenotettava hyötynäkökulma. Aktivoitumisen osuutta voidaan arvioida maailmalla yleisesti käytössä olevien nettiäänestysjärjestelmien arviolta korkeintaan parin prosenttiyksikön aktivoitumistekijällä. Näin on nähty tilanteen olevan mm. Virossa. Norjassa nettiäänestyskokeilun seurauksena arvioitiin, että havaittavaa aktivoitumista äänestämisessä ei tapahtunut.

Yhtenä merkittävänä hyötynä nettiäänestysjärjestelmän käyttöönotossa voidaan nähdä yleensä neuvoa-antavan kunnallisen kansanäänestyksen mahdollistuminen. Nettiäänestystyöryhmän työpajoissa[14] on käynyt ilmi, että nykyään on suurilla kaupungeilla vaikeuksia järjestää kunnallisia kansanäänestyksiä taloudellisten ja ajallisten rajoitteiden takia. Nettiäänestysjärjestelmä saattaisi mahdollistaa näissä tapauksissa yleensä kunnallisen kansanäänestyksen ja siten lisätä demokratiaa merkittävästi.

Nettiäänestysjärjestelmä hyvin suunniteltuna ja toteutettuna mahdollistaisi helpomman äänestämisen esteellisille henkilöille. Samoin hyvin suunniteltu ja toteutettu järjestelmä

[11] vaalit.fi

[12] Oikeusministeriön kustannuslaskelmat vaaleista 1999-2012

[13] Helsingin kaupungin kululaskelma vaaleista 2008-2012

[14] Työpajat, katso osallistujat liitteestä.

mahdollistaisi äänestämisen myös ns. virka-ajan ulkopuolella ja siten helpottaen äänestämistä henkilöiltä, jotka eivät pääse äänestyspaikalle. Toki kunnallisen kansanäänestyksen kirjeäänestys mahdollistaa äänestämisen ilman äänestyspaikalla käyntiä, mutta nettiäänestys saattaa helpottaa äänestystapahtumaa.

Huomattavaa on, että yksi yhteinen järjestelmä, joka tukisi nettiäänestystä Suomessa saattaisi tuottaa hyötyjä myös muiden järjestöjen käyttämänä kuin pelkästään kuntien apuna. Järjestöt ja yhdistykset saattaisivat käyttää järjestelmää omissa vaaleissaan ja siten kattaa osan järjestelmän kuluista käyttömaksujen kautta. Samoin olemassa olevan järjestelmän käyttäminen näissä järjestöjen ja yhdistysten vaaleissa hyödyttäisi merkittävästi järjestöjä ja yhdistyksiä sisäisen demokratian parantamisessa ja jäsenten käyttäessä tuttua järjestelmää ei erillistä käyttöohjeistusta välttämättä tarvitsisi, ainakaan ei kovin massiivisessa mielessä.

Varsinaisia vaaleja tukeva nettiäänestysjärjestelmä myös ulkosuomalaisille sopivan tunnistusmekanismin kautta saattaisi mahdollistaa ulkomailla asuvien helpomman äänestämisen.

Kustannukset

Mahdollisen nettiäänestysjärjestelmän kustannuksia arvioidessa keskitytään tässä neuvoa-antavan kunnallisen kansanäänestyksen mahdollistavaan järjestelmään. Nettiäänestysjärjestelmä, joka kykenee hoitamaan yleiset vaalit, on tietoturvavaatimuksiltaan vaativampi ja kustannusten arviointi tässä vaiheessa on vaikeaa. Nettiäänestystyöryhmän työ on suurelta osin keskittynyt nimenomaan kunnallisen kansanäänestyksen mahdollistamaan järjestelmään.

Kustannustekijöitä

Tässä keskitytään muutamaan erilaiseen järjestelmään, joista on keskusteltu nettiäänestystyöryhmän työpajoissa[15]. Kunnallisen kansanäänestyksen mahdollistavat järjestelmiä voidaan tutkia seuraavilla eri kompleksisuuden asteilla:

1. Pelkkä tunnistus, äänestys tapahtuu vain kerran ennakkoon kirjeäänestyksen kanssa samanaikaisesti tai aikaisemmin, ei äänestystä varsinaisena äänestyspäivänä
2. Pelkkä tunnistus, äänestys tapahtuu mahdollisesti useasti, viimeinen ääni huomioidaan, ennakkoon kirjeäänestyksen kanssa samanaikaisesti tai aikaisemmin, ei äänestystä varsinaisena äänestyspäivänä

[15] Työpajat, katso työhön vaikuttaneet liitteestä.

3. Kuten 2, mutta äänestys myös äänestyspäivänä netin kautta
4. Sama kuin 1, mutta mukana äänestäjän äänen allekirjoitus
5. Sama kuin 2, mutta mukana äänestäjän äänen allekirjoitus
6. Sama kuin 3, mutta mukana äänestäjän äänen allekirjoitus

Äänestäjän äänen sähköinen allekirjoitus tuo mukanaan vaatimuksen tunnistautumismenetelmästä, joka tarjoaa myös vahvan allekirjoituksen. Tällä hetkellä Suomessa on sähköisen allekirjoituksen mahdollistavia tunnistusmenetelmiä mobiilitunniste ja sähköinen henkilökortti. Nykytilanteessa kummankaan käyttöaste väestössä ei ole riittävä, että niitä voisi käyttää yleisesti ainoina allekirjoitusmenetelminä. Sähköisen allekirjoituksen mahdollistavan taustajärjestelmän kustannukset, joihin ei tämän tarkemmin oteta kantaa, voidaan olettaa olevan nykyisen sähköisen henkilökortin kustannusten luokkaa, eli kymmenen euron suuruusluokkaa vuositasolla äänioikeutettua kohden.

Teknisesti sähköinen allekirjoitus tuo jonkin verran lisäkustannuksia järjestelmään, lähinnä lisääntyneiden äänestäjän päätelaitteen ohjelmiston toiminnallisuusvaatimusten myötä. Taustajärjestelmän, eli sähköisen allekirjoituksen mahdollistavan yleisen tunnistusjärjestelmän, myötä tulevia kuluja on hankala arvioida, mutta niiden suuruusluokka lienee edellä esitetty. Oheisessa analyysissä nämä kulut on jätetty huomiotta, koska ne eivät suoraan liity nettiäänestysjärjestelmän kuluihin. Koska sähköisen allekirjoittamisen myötä tulevat kulut varsinaisen nettiäänestysjärjestelmän osalta mahtunevat kustannusarvioiden virherajoihin, voidaan käsitellä yllä olevista vaihtoehdoista 1-3 ja todeta vaihtoehdoista 4-6, että niiden lisäkustannukset eivät varsinaisesti tule nettiäänestysjärjestelmästä vaan taustajärjestelmästä. Lisäkustannukset suoraan nettiäänestysjärjestelmään toteutetusta sähköisestä allekirjoituksesta ja henkilön salauksesta mahtunevat kustannusarvioiden virherajoihin joka tapauksessa.

Jos tyydytään nettiäänestysjärjestelmässä pelkkään äänestäjän tunnistautumiseen ilman äänestäjän äänen allekirjoittamista, saadaan yksinkertaisimmillaan tehtyä nettiäänestysjärjestelmä, jonka mallina voisi toimia nykyinen kansalaisaloite.fi-tyyppinen palvelu. Ko. palvelussa tunnistaudutaan VETUMA:n tarjoamilla tavoilla ilman allekirjoituksia. Kyseisessä palvelussahan kannatetaan jotain aloitetta ja teknisessä mielessä tuo kannatus toimii samantyyppisesti kuin kuntalaisen kansanäänestyksessä. Joitain muutoksia pitää tietenkin ohjelmiston logiikkaan tehdä, mutta perustoiminnoiltaan yksinkertaisin kunnallinen kansanäänestys voitaisiin toteuttaa hyvin lähellä kansalaisaloite.fi-palvelun toiminnallisuutta. Tällöin olisi ko. järjestelmän kustannukset suuruusluokaltaan kaksinkertaiset kansalaisaloite.fi -palvelun kustannuksista sekä hankintakustannuksiltaan että käyttökustannuksiltaan. Tällöin järkevin lähestymistapa ohjelmiston tuottamiseen lienee ohjelmiston teettäminen. Valmiin,

vaaleihin keskittyneen, tuotteen räätälöiminen ei liene kovin kannattavaa, johtuen valmiisiin vaalijärjestelmiin rakennetusta korkeammasta tietoturvallisuudesta (vaalien vaatimusten mukaisesti), joka johtaa tuotteen korkeaan hankintahintaan.

Vaihtoehtoiset toteutukset

Edellä esitetyistä vaihtoehdoista edullisin toteuttaa (pienin toiminnallisuus) on vaihtoehto 1. Kuten edellä todetaan, kustannus erillisenä järjestelmänä on suuruusluokaltaan kaksi kertaa kansalaisaloite.fi-palveluun verrattuna. Toiminnallisesti tarvitsee järjestelmän yhden aloitteen kannattamisen sijasta tarjota useaa vaihtoehtoa, joista äänestäjä voi kannattaa vain yhtä (yhtenä vaihtoehtona mukana myös "tyhjä"). Lisäksi järjestelmä tarvitsee taustalle äänestysrekisterin hallinnan. Tunnistautumisen lisäksi tarvitaan äänestäjän vertaaminen äänestysrekisteriin, että saadaan selville, onko äänestäjä oikeutettu äänestämään juuri ko. kansanäänestyksessä. Äänet järjestelmässä tallennetaan äänestyksen (palvelimen) salaisella avaimella salattuina aina vaalien laskemisen alkuun saakka (“uurna”).

Vaihtoehto 2 tuo mukanaan toiminnallisuuden muutoksen taustajärjestelmään, "palvelimiin". Taustajärjestelmän täytyy kyetä identifioimaan äänestäjän antama ääni ja huomioimaan ääntenlaskennassa vain viimeisin nettiääni tai muuten validi ääni, esimerkiksi paperilla viranomaisen läsnäollessa annettu ääni, jos on säädetty lippuäänen olevan “vahvempi”. Tämä toiminnallisuus vaatii taustajärjestelmään “uurnan”, joka tallentaa samaan tilaan äänestäjän identiteettitiedon ja varsinaisen äänen ja siten poikkeaa hiukan toiminnallisuudeltaan vaihtoehto 1 uurnasta. Päätelaitteessa tarvitaan mahdollisesti lisätoiminnallisuutta äänestystapahtuman hyvin sujumiseen. Tämä ylimääräinen toiminnallisuus pitää huomioida mahdollisesti kustannuksia lisäävänä tekijänä.

Vaihtoehto 3 tuo mukanaan merkittävän monimutkaisuusasteen. Monimutkaisuutta vaihtoehto 3 tapauksessa nostaa nimenomaan järjestelmän hyvin korkea saavutettavuus, koska äänestyspäivänä saavuttamaton järjestelmä on erittäin epätoivottava asettaen äänestämisen tasavertaisuuden kyseenalaiseksi. Tarpeeksi korkean saavutettavuuden järjestelmä pystytään käytännössä takaamaan vain järjestelmän kahdentamisen kautta, jolloin itse laitekustannukset, sekä hankinta että ylläpito, nousevat vähintään kaksinkertaisiksi ottaen huomioon myös kahdennetut verkkoyhteydet.

Yllä oleva pitää kaikilta osiltaan paikkaansa myös allekirjoituksen mahdollistavissa järjestelmissä, eli mitä enemmän toiminnallisuutta järjestelmään ladataan, sitä suuremmat kustannukset järjestelmästä syntyvät. Allekirjoituksen myötä kaikissa vaihtoehdoissa tulee merkittävästi lisätoiminnallisuutta päätelaitteen ohjelmistoon, sillä ääni pitää allekirjoittaa

nimenomaan päätelaitteessa. Päätelaitteen ohjelmiston pitää pystyä tukemaan allekirjoituksen menetelmää, mikä tekninen menetelmä sitten onkaan.

Varsinaisten vaalien yhteydessä täytyy asettaa korkeammat vaatimukset vaalin oikealle sujuvuudelle, kuten tietoturvaa käsittelevässä osiossa todettiinkin. Neuvoa-antavan kansanäänestyksen yhteydessä on huomioitava, että virhetilanteen tai väärinkäytön ilmaantuessa voidaan arvioida, voidaanko kansanäänestyksen tulosta pitää luotettavana ja vastaavasti ottaa tämä huomioon kansanäänestyksessä ollutta päätöstä tehdessä. Kyseessähän on neuvoa-antava kansanäänestys, joka ei sido poliittisia päättäjiä ehdottomasti. Koska varsinaiselle vaalille on korkeammat vaatimukset jokaisen äänen oikeinlaskemiselle, on vaaleissa käytettävän nettiäänestysjärjestelmän tietoturvan rakentamiseen käytettävä merkittävästi enemmän resursseja ja myös järjestelmän monitoroinnin täytyy olla huomattavan korkealla tasolla.

Taulukko kustannusten jakaumasta eri osioille (arvio)

Järjestelmä	Hankinta	Ylläpito/vuodessa	Operointi/vuodessa
1.Kansalaisaloite + äänirekisteri	X	X/6	100 k€
2. 1+päätelaiteohjelmiston muutokset + tietoturvallinen uurna	1.5 * X = Y	Y/6	100 k€
3. 2+kahdennus+korkea käytettävyys	3.25 * X = Z	Z/6	200 k€

Edellä olevassa taulukossa on arvioitu eri vaihtoehtojen keskeistä suuruusluokkaa. Ylläpidon kustannusten on arvioitu olevan noin 15% (⅙) hankintahinnasta. Ylläpito sisältää ohjelmiston ylläpidon, virhekorjaukset ja mahdolliset pienet muutokset. Palvelinten hosting-kulut ja ylläpito, kuten myös verkon ylläpito ja palvelut kuuluvat myös ylläpitoon. Operointi sisältää varsinaiset henkilökulut järjestelmän operoinnissa ja monitoroinnin kulut. Mahdollisten salausavainten hallinta ja kansanäänestyksen perustaminen kuuluu operointikuluihin. Kahdennetun järjestelmän (vaihtoehto 3) operointi on kaksinkertainen muihin verrattuna äänestyspäivien korkean saavutettavuuden vaatimuksen vuoksi.

Äänten allekirjoituksen kustannus kuhunkin kulukategoriaan on arviolta ylimääräinen 1.2 kerroin ilman taustajärjestelmäkuluja. Taustajärjestelmäksi siis tarvitaan allekirjoituksen mahdollistava

vahva tunnistautumisjärjestelmää kansalaisille laajalti käyttöön. Alla olevassa taulukossa ei käsitellä tätä 20% lisäystä erikseen, vaan käsitellään ainoastaan edellä luetellut vaihtoehdot 1-3.

Kuten hyötyjä käsittelevän kappaleen alussa on hyvin karkeasti arvioitu, voidaan neuvoa-antava kunnallinen kansanäänestyksen mahdollistava nettiäänestysjärjestelmä taloudellisesti perustella, jos äänioikeutetun yhden äänestyksen keskimääräinen kustannus jää alle 4€ kokonaisuudessaan. Kuntien kannalta voidaan ajatella, että järjestelmä on taloudellisesti perusteltavissa joka tapauksessa, jos nettiäänestystyöryhmässä esitetty ajatus nettiäänestysjärjestelmän tarjoamisesta valtion toimesta kunnille toteutuu valtion kantaen kustannukset järjestelmästä. Tällöin kuntien kustannukset kansanäänestyksestä oleellisesti vähentyvät niiden äänien osalta, jotka tulevat nettiäänestysjärjestelmän kautta.

Esimerkin kautta on varman selkeintä käydä läpi kulurakennetta. Kun oletamme

- useita kansanäänestyksiä käynnissä samanaikaisesti
- hankintakustannus 600 000 euroa
- oletettu ylläpito 100 000 euroa vuodessa
- operointikulut 100 000 euroa vuodessa, kaksinkertaiset kahdennetulla korkean käytettävyyden järjestelmällä
- 5 vuoden investoinnin kuoletusaika (5 v sisällä hankitaan uusi nettiäänestysjärjestelmä)
- Järjestelmän käyttö säästää yhtä ääntä kohden puolet äänestyksen kuluista. Edellä arvioitiin maksimikuluiksi kansanäänestyksestä saman kuin kunnallisvaaleissa ääntä kohden kulut eli 4 euroa/ääni.

Äänestyksen kuluista voidaan olettaa, että maksimikustannus/ääni ei toteudu, koska useissa kansanäänestyksissä saadaan optimoitua prosessit kohdalleen. Tällöin yhden äänestystapahtuman valvonta- ja laskentakustannukset ovat pienet, varsinkin jos nettiäänestys saavuttaa huomattavan suosion. Käytetään laskennallisena arviona 75% maksimista eli noin 3 euroa/ääni. Tällöin nettiäänestysjärjestelmän tuoma säästö on sitä kautta äänestäessä 1,5 euroa/ääni.

Yllä olevan listan oletuksilla saadaan yhden vuoden laskennallisiksi kuluiksi järjestelmällä 2 430 000 euroa vuodessa nettiäänestysjärjestelmästä. Tällöin päästään “nollatulokseen” taloudelliselta kannalta, jos äänestäjiä on kunnallisissa neuvoa-antavissa kansanäänestyksissä nettiäänestysjärjestelmän kautta enemmän kuin 290 000 äänestäjää vuodessa.

Järjestelmällä 3 tulee vastaavilla oletuksilla nollatuloksen vaatimukseksi enemmän kuin 610 000 äänestäjää nettiäänestysjärjestelmän kautta vuositasolla.

			Vuosikulut			
Järjestelmä		Hankintahinta	Hankinta, kuoletus	Ylläpito	Operointi	Ääntä vuodessa
1. Pelkkä tunnistus, äänestys tapahtuu vain kerran ennakkoon kirjeäänestyksen kanssa yhtäaikaa tai aikaisemmin, ei äänestystä varsinaisena äänestyspäivänä	0%	600 000 €	120 000 €	100 000 €	100 000 €	210 000
	+30%	780 000 €	156 000 €	130 000 €	130 000 €	270 000
	-30%	546 000 €	84 000 €	70 000 €	70 000 €	150 000
2. Kuten vaihtoehto1, mutta lisättynä mahdollisuus äänestää useasti nettiäänestyksenaikana	0%	900 000 €	180 000 €	150 000 €	100 000 €	290 000
	+30%	1 170 000 €	234 000 €	195 000 €	130 000 €	380 000
	-30%	819 000 €	126 000 €	105 000 €	70 000 €	200 000
3. Kuten vaihtoehto 2, mutta äänestys myös mahdollista äänestyspäivänä	0%	1 950 000 €	390 000 €	325 000 €	200 000 €	610 000
	+30%	2 535 000 €	507 000 €	422 500 €	260 000 €	790 000
	-30%	1 774 500 €	273 000 €	227 500 €	140 000 €	430 000

Taulukossa edellä on esitetty eri vaihtoehtojen kustannukset ja kustannusten ±30% vaihteluväli. Hankintahinta on varsinainen hankintahinta ja sitten on myös esitetty vuotuinen kuoletuskustannus 5 vuoden kuoletusajalla. Ylläpito on noin 15% ja operointi 100 000 €, kahdennetulla järjestelmällä 200 000 €. Ääntä vuodessa -sarake esittää ns. äänestämisen break-even arvon eli äänien määrän järjestelmän kautta, jolloin järjestelmän tuomat säästöt ovat samat kuin kustannukset. Jos järjestelmän kautta äänestää enemmän äänioikeutettuja vuodessa, säästöt ovat suuremmat kuin kustannukset.

Varsinaiset vaalit mahdollistavan järjestelmän kustannukset halvimmillaankin voidaan arvioida olevan useita kertoja pelkän neuvoa-antavan kunnallisen kansanäänestyksen järjestelmän kustannukset. Suurin tekijä kustannuksista tulee tiukemmista tietoturvavaatimuksista ja järjestelmän korkeammasta monitoroinnin tasosta. Käytännössä varsinaisten vaalien nettiäänestysjärjestelmää ei voida kustannustehokkaasti rakentaa laajentaen neuvoa-antavan kunnallisen kansanäänestyksen nettiäänestysjärjestelmää tietoturvavaatimusten kasvamisen vuoksi. Kustannusten vuoksi ei kannata rakentaa korkean tietoturvan järjestelmää, ellei se ole ehdottoman välttämätöntä.

Huomattavaa kustannuslaskelmissa on, että kustannusten suuri erilaisuus järjestelmissä, jotka tukevat yleisiä vaaleja ja jotka kykenevät vain neuvoa-antavaan kansanäänestyksen tukemiseen, aiheuttaa lähes automaattisesti näiden eri järjestelmien erottamisen toisistaan. *Yleisen vaalin kustannukset tulevat olemaan aivan eri kokoluokkaa, johtuen lähinnä korkeampien tietoturvavaatimusten täyttämisestä verrattuna neuvoa-antavan kansanäänestyksen vaatimuksiin.*

Kuten tietoturvakappaleen teksti osoittaa on kansanäänestykselle ja yleisille vaaleille asetettava erilaiset vaatimukset. On vaikea nähdä järkeväksi rakentaa yhteinen järjestelmä, jota voidaan käyttää erilaisilla prosesseilla ja joka pystyy tukemaan erilaisten prosessien toiminnallisuutta. Varsinkin mahdollinen tilanne, jossa samanaikaisesti on järjestelmässä käynnissä kymmeniä kansanäänestyksiä, joita kaikkia pitäisi tukea yleisten vaalien tietoturvaan keskittyvällä järjestelmälle, aiheuttaa tarpeetonta kompleksisuutta järjestelmän suunnittelulle ja ylläpidolle. Tämä lisää kustannuksia kansanäänestysten järjestelmälle tarpeettomasti.

Nettiäänestysjärjestelmä myös voisi parantaa ja lisätä kansalaisten osallistumista demokraattiseen päätöksentekoon. Tästä antaa viitteitä otakanta.fi- ja kansalaisaloite.fi-palveluiden nopeasti kasvanut suosio. Tämän lisääntyneen osallistumisen arvoa on hyvin vaikeata verrata järjestelmän kehitys- ja ylläpitokustannuksiin.

Erityisesti nettiäänestysjärjestelmä mahdollistaisi kunnallisten kansanäänestysten toteuttamisen Helsingissä ja muissa suurissa kaupungeissa. Tämä on selvästi arvokas asia, mutta euromääräisen arvon arviointi ei ole tämän esiselvityksen keinoin tehtävissä.

Laatutavoitteet

Nettiäänestysjärjestelmän laatutavoitteet ovat korkealla. Korkean laadun perusteena on äänestyksen luotettavuuden takaaminen ja nettiäänestysjärjestelmän hyväksymisen parantaminen.

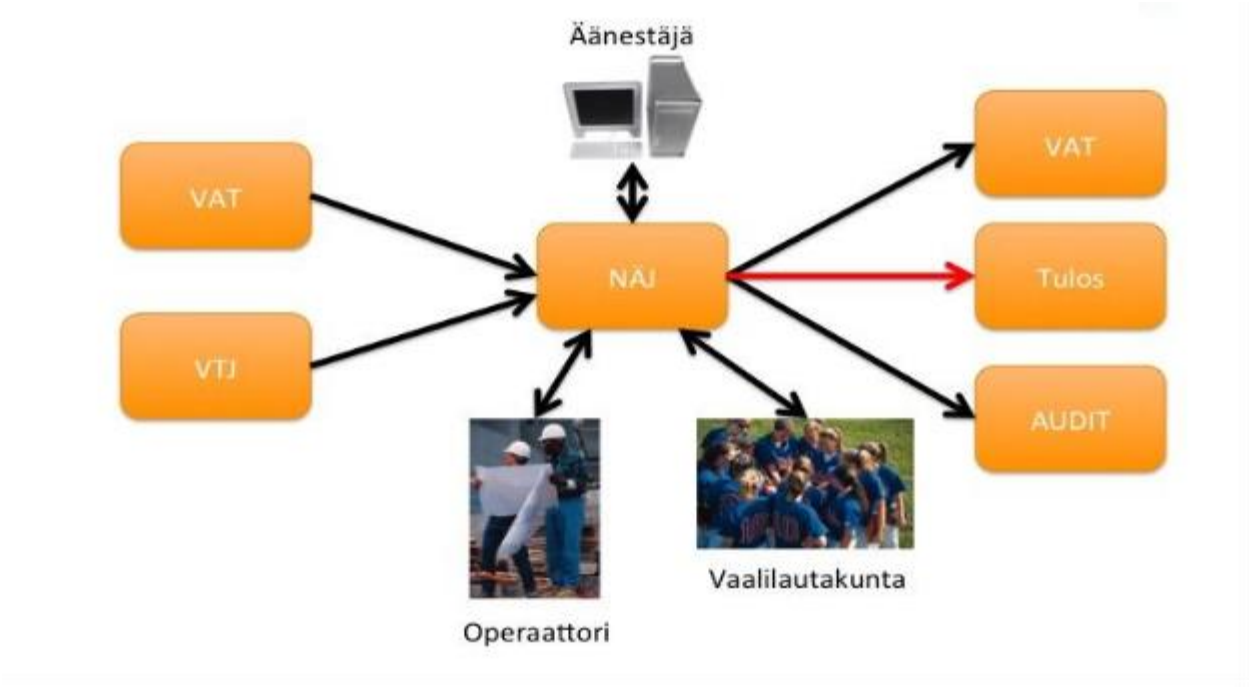
Korkealla laadulla varmistetaan äänestäjien järjestelmän hyväksyminen ja tulosten oikeellisuus äänestystapahtumassa. Korkean laadun takeena järjestelmässä toimii mahdollisimman laaja ja hyvin tuettu auditointi sekä järjestelmän kehittämisen että käytön aikana. Kaikkiin järjestelmän osiin ja toiminnallisuuksiin pitää pystyä tutustumaan vapaasti ja siten mahdollisimman pitkälle taataan ohjelmiston toiminnan luotettavuus.

Toki pelkästään auditoinnilla ei taata ohjelmiston luotettavaa ja laadukasta toimintaa. Laadukkaan ohjelmiston takana on aina laadukas ja jäljitettävissä oleva ohjelmistonkehitys. Ohjelmistonkehityksen laadun takaa jäljitettävä vaatimustenhallinta ja vaatimusten tarkka analyysi, myös sivuvaikutusten analyysi. Tämä ei tietenkään estä tekemästä ohjelmistonkehitystä ketterää kehityksen keinoin, ainoastaan vaatii vaatimusten analysoinnin tarkemmin kehityksen vaiheessa, jossa vaatimuksista keskustellaan.

Suljetulla kehityssyklillä laadukkaan ohjelmiston toteuttaminen on vaikeaa, ainakin sen laadun varmentaminen on vaikeaa. Ohjelmiston laatuun ja toimintaan on vaikea uskoa ilman riippumattomien auditoijien raportointia.

Integrointi muihin järjestelmiin

Nettiäänestysjärjestelmä tarvitsee toimiakseen useita yhteyksiä muihin ympäröiviin järjestelmiin. Näiden järjestelmien integrointi takaa nettiäänestyksen sujuvan toimittamisen.



Kuva 2. Nettiäänestysjärjestelmän liitännät muihin järjestelmiin

Vaalitietojärjestelmä (VAT)

Nettiäänestysjärjestelmä voi ottaa vaalitietojärjestelmästä toiminnallisuutena äänestys- ja kuntajaotuksen sekä äänestysoikeusrekisterin. Vaalitietojärjestelmä tuottaa nämä listat palveluna jo varsinaisiin vaaleihin, joten kunnallisia kansanäänestyksiä varten näiden toimittaminen olisi helppoa ja joustavaa. Tulosten julkistamisen kannalta on vaalitietojärjestelmässä jo valmiit toiminteet ja prosessit näitä varten. Vaalitietojärjestelmän käyttö ei ehkä ole järkevintä pienten kuntien kansanäänestysten toimittamisessa, jolloin kustannuksiltaan vaalitietojärjestelmä ei välttämättä ole järkevä vaihtoehto. Samoin ei vaalitietojärjestelmä pysty nykyisessä muodossaan ilman lisäinvestointeja toimittamaan useita kymmeniä samanaikaisia kansanäänestyksiä, jotka alkavat ja loppuvat eri aikoihin.

Jos nettiäänestysjärjestelmää laajennetaan varsinaisiin yleisiin vaaleihin, on vaalitietojärjestelmän käyttö käytännössä pakollista vaalien äänioikeuden yhtenäisyyden takaamiseksi. Ei ole nähtävissä, että vaalien lippuäänestys- ja nettiäänestysrekisteri hoidettaisiin erillisillä järjestelmillä.

Väestötietojärjestelmä (VTJ)

Kunnallisen kansanäänestyksen tapauksessa voidaan todeta, että nettiäänestysjärjestelmä voisi toteuttaa kevennetyn version vaalitietojärjestelmän toiminnasta ja täten ei kunnallisten neuvoa-antavien kansanäänestysten yhteydessä olisi tarvetta käyttää vaalitietojärjestelmää. Tällöin äänioikeusrekisterin tiedot ylläpidettäisiin nettiäänestystietojärjestelmän sisäisesti. Tarvittavat tiedot haetaan tällöin suoraan VTJ:stä samojen prosessien kautta kuin vaalitietojärjestelmä nykyään. Neuvoa-antavan kansanäänestyksen yhteydessä ei ole tarvetta järjestää maistraattiin tietoyhteyttä (kuten vaalitietojärjestelmässä on) tietojen korjaamista varten äänestysprosessin aikana, joten äänestysrekisterin ylläpitoon nettiäänestysjärjestelmässä ei tarvita erikoista ylläpitoliittymää.

VTJ-liittymä olisi käytössä vain kansanäänestyksen perustamisvaiheessa, kun tiedot haetaan äänestysalueista ja äänioikeutetuista nettiäänestysjärjestelmään. Nettiäänestysjärjestelmän pitää kyetä ylläpitämään tällöin tiedot äänestäneistä äänestyksen aikana. Erillistä äänestysoikeusrekisteriä järjestelmän ulkopuolella ei olisi käytettävissä. Nettiäänestysjärjestelmän tulisi kyetä tukemaan myös neuvoa-antavan kansanäänestyksen kirjeäänestystä ja paperiäänestystä äänestysoikeusrekisterin kannalta.

Yleisissä vaaleissa ei VTJ-yhteyttä tarvita, sillä vaalitietojärjestelmän tulee kyetä tarjoamaan tarvittavat palvelut nettiäänestysjärjestelmälle ja vaalitietojärjestelmä on joka tapauksessa käytössä yleisissä vaaleissa.

VETUMA

Äänestäjän ja vaalivirkailijoiden tunnistautumiseen tarvitaan nykyään VETUMA-yhteys. VETUMA tarjoaa erilaisia tunnistautumismenetelmiä nettiäänestysjärjestelmän käyttöön.

Keskusteluissa asiantuntijoiden[16] *kanssa on todettu, että VETUMAn tarjoamat pankkitunnuksiin pohjautuvat tunnistautumisjärjestelmät eivät ole tällä hetkellä tarpeeksi toiminnalliset yleisiä vaaleja varten nettiäänestyksessä. Pankkitunnistautumisen ongelmalliseksi puoleksi on todettu vahvan sähköisen allekirjoituksen puute (ainoastaan tunnistautuminen on mahdollista), jolloin äänestystapahtuman eheyden varmentaminen on hankala toteuttaa. Yleisissä vaaleissa on käytettävä vahvoja allekirjoituksen menetelmiä, kuten sähköistä henkilökorttia tai mobiilivarmennetta, kun vaalisalaisuus ja eheys halutaan varmentaa. Vaalivirkailijoilla riittänee yleisissäkin vaaleissa pelkkä tunnistautuminen, jolloin pankkitunnusten käyttö olisi tarpeeksi*

[16] Työpajat, katso työhön vaikuttaneet liitteessä.

vahva menetelmä. Vaalivirkailijoiden salaukseen voidaan tarvittaessa käyttää vaalivirkailijoille erikseen jaettavia salausmenetelmiä, jotka eivät ole VETUMAn piirissä.

VETUMA-liityntä järjestelmässä tulee äänestäjillä äänestäjien päätelaitteiden kautta ja vaalivirkailijoilla nettiäänestysjärjestelmän kautta.

Operointijärjestelmät

Järjestelmän operoijat joutuvat liittymään järjestelmään operointijärjestelmien kautta. Nettiäänestysjärjestelmän toimittaja kykenee toimittamaan operointijärjestelmätkin, joten ne on katsottava osaksi nettiäänestysjärjestelmää, eikä ulkoisiksi järjestelmiksi.

Monitorointi

Nettiäänestysjärjestelmän toiminnan valvomiseksi pitää järjestelmää monitoroida nettiäänestysjärjestelmän pystyttämisestä lähtien järjestelmän sulkemiseen saakka. Järjestelmän operoijilla ei tule olla mitään pääsyä monitorointijärjestelmiin. Tällä varmistetaan monitoroinnin riippumattomuus. Monitorointijärjestelmästä ei myöskään saa vuotaa minkäänlaista tietoa takaisin nettiäänestysjärjestelmään, ainoastaan määrämuotoiset lokitusviestit nettiäänestysjärjestelmästä monitorointiin on sallittava.

Monitorointijärjestelmän lokien on oltava teknisesti vain kerran kirjoitettavia, muuten lokien yhtenäisyys vaarantuu.

Äänestäjän päätelaitteet

Päätelaitteen pitää pystyä toimittamaan äänestyksen tarvitsemat toimenpiteet ilman, että äänestystapahtuma vaarantuu. Päätelaitteen tulee pystyä yleisten vaalien tapauksessa allekirjoittamaan ääni ja salaamaan se. Äänestäjän pitää pystyä äänestystapahtuman jälkeen varmistamaan äänensä perillemeno oikein ja muuttumattomana. Äänestäjien päätelaitteet eivät ole valtiollisen hallinnan tai ylläpidon alaisia.

Äänestäjän päätelaitteen tietoturvan varmentaminen ja äänestystapahtuman eheyden suojeleminen ei nykyään ole mitenkään helppo tehtävä, kuten tietoturvaa käsittelevässä osassa todettiin. Nettiäänestystyöryhmä on lähtenyt päätelaiteriippumattomuudesta, mutta siihen liittyy rajoitteita, kuten aikaisemmista tekstistä on käynyt ilmi. Päätelaiteriippumattomuus ei ole välttämättä mahdollista kaikissa tapauksissa, varsinkaan mahdollisen äänen allekirjoittamisen yhteydessä.

Kilpailutuksen perusteet ja markkinakartoitus

Esiselvityksessä syntyneen ymmärryksen mukaan nettiäänestysjärjestelmä on mahdollista toteuttaa vain avoimena järjestelmänä. Järjestelmän lähdekoodin on oltava kaikkien kiinnostuneiden vapaasti tutkittavissa ja auditoitavissa. Mikäli järjestelmässä on suljettuja osia, luottamus järjestelmän toiminnallisuuteen ja tietoturvallisuuteen on lähtökohtaisesti heikko, mikä on omiaan vähentämään järjestelmän käyttöä.

Keväällä 2014 tehdyssä teknisessä vuoropuhelussa mukana olleet toimittajat olivat keskittyneet kehittämään *vaaleihin soveltuvia järjestelmiä.* Nämä järjestelmät luonnollisesti täyttävät kansanäänestysten vaatimukset, mikäli ne vain ovat luontevasti muokattavissa kansanäänestyksiin soveltuviksi. Tämä on luultavaa, mutta vaatii joko järjestelmän toimittajalta tai Suomen valtion kilpailuttamalta ohjelmistotoimittajalta tarkemmin määrittelemättömän määrän työtä.

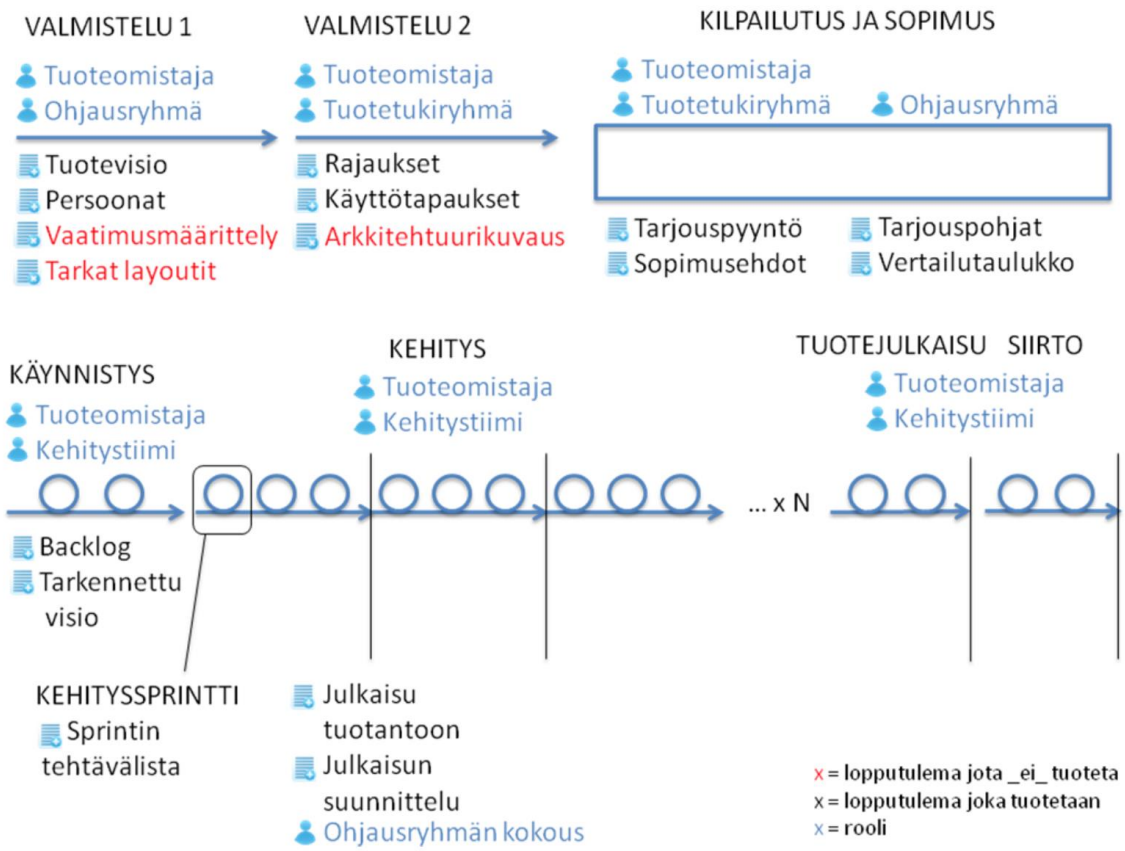
Tekniseen vuoropuheluun osallistuneista toimittajista yksikään ei vuoropuhelun aikana ollut halukas avaamaan järjestelmänsä koko lähdekoodia. Toimittajat perustelivat tätä liikesalaisuuksilla. Sittemmin ainakin Norjassa järjestelmän toimittanut järjestelmätoimittaja on suostunut lähdekoodin avaamiseen. Suomen valtion on pidettävä koodin avoimuutta ehdottomana vaatimuksena nettiäänestysjärjestelmän kilpailutuksessa.

Kuvan 1 mukaisen nettiäänestysjärjestelmän kustannukset riippuvat tietoturvasta ja toiminnallisuuksien laajuudesta aiemmin kuvatulla tavalla. Jos Suomen valtio päätyy hankkimaan mahdollisimman suppean - nykyisen kirjeäänestyksen korvaavan ja tasoisen - järjestelmän, niin järjestelmä on mahdollista toteuttaa räätälöitynä ratkaisuna. Ohjelmiston kehittämiseen kykeneviä ohjelmistoyrityksiä on Suomessa lukuisia.

Nettiäänestysjärjestelmän kehitystyötä ei ole välttämättä pakko ostaa vain yhdeltä ohjelmistotoimittajalta. Järjestelmä on syytä kehittää ketterin kehitysmenetelmin. Tällöin Suomen valtio kilpailuttaisi tekijöitä heidän osaamisensa (ja tuntihintansa) perusteella, ei kokonaisen nettiäänestysjärjestelmän toteutusprojektia.

Ketterä kehittäminen on suositeltavaa koska silloin mahdolliset virheet ja väärinymmärrykset ja lakimuutokset on helpompi ottaa huomioon, koska järjestelmää on mahdollista koestaa ja testata usein, jokaisen sprintin jälkeen.

Seuraava kuva kuvaa ketterän hankinnan vaiheet. On huomattava, että hankinnan - ja myös kehitysprojektin - onnistumisen kannalta on olennaisen tärkeää kokopäiväisen tuoteomistajan nimittäminen heti hankinnan alkuvaiheessa.



Tämä esiselvitys ei ole osa kuvassa kuvattua prosessia. Tätä esiselvitystä voisi kutsua vaiheeksi “Valmistelu 0”.

Ketterään toteutustiimiin on syytä palkata käytettävyyssuunnittelija, käyttöliittymän toteuttaja ja tietokanta-asiantuntija tavanomaisten järjestelmäkehittäjien lisäksi. Lisäksi on palkattava - tai hankittava vaikkapa virka-apuna puolustusvoimista - tietoturva- ja kryptologia-asiantuntijoita, vaikka varsinaisia ohjelmiston krypto-osioita ei kannatakaan kehittää omin voimin vaan käyttää valmiita osioita luotettavalta taholta hankittuna. Toteutustiimin kooksi voidaan alustavasti arvioida noin 5-7 henkilöä.

Toteutustiimin lisäksi on syytä ostaa palveluna tietoturvatestausta. Järjestelmän tietoturvallisuudesta on mahdollista varmistua vain, jos toteutusta testataan toteutustiimin ulkopuolisin voimin säännöllisin väliajoin. On suositeltavaa ostaa tämä työ palveluna vaikkapa samalta tutkimusryhmältä, joka arvioi Viron järjestelmän tietoturvan ja totesi sen puutteelliseksi.

Koska järjestelmä jää valtion omistukseen ja käyttöön (oikeusrekisterikeskuksen eli ORK:n), niin ORK:n on palkattava tai muuten hankittava palvelukseensa riittävästi osaavia ihmisiä järjestelmän jatkokehityksen ohjaamiseen ja tietoturva-asioiden ratkaisemiseen ja

huomioimiseen. Tämä siksi, että järjestelmän kehitystä ei voi lopettaa, mutta ostetuin voimavaroin ei voi jatkaa loputtomiin; on oltava omaa osaamista jo pelkästään ostamisen osaamiseksi. Näin ORK toimii myös vaalitietojärjestelmän kehityksen kanssa.

Kansanäänestysjärjestelmää ei voi jälkikäteen laajentaa vaalijärjestelmäksi. Vaalijärjestelmän kehittämisen kilpailuttaminen on huomattavasti vaikeampaa kuin kansanäänestysjärjestelmän. Mikäli jokin markkinoilla olevista vaalijärjestelmistä todetaan riittävän tietoturvalliseksi, on sen hankkiminen luonnollisesti mahdollista. Vaalijärjestelmän - valmisohjelmistona - kilpailuttamiseen ei tässä esiselvityksessä paneuduta tämän tarkemmin, koska kilpailutus ei poikkea suuresti minkään muun valmisjärjestelmän kilpailuttamisesta.

Suunnitelma toteutus- ja käyttöönottovaiheelle

Nettiäänestysjärjestelmän toteutusvaiheeseen siirtyminen vaatii erilaisia pilotointeja järjestelmän toiminnallisuudesta ja selkeää keskustelua järjestelmän lopullisesta tavoitteesta. Jos nettiäänestysjärjestelmän halutaan toteuttavan yleisen vaalin myös neuvoa-antavan kansanäänestyksen lisäksi, pitää järjestelmän tietoturvataso nostaa korkealle tasolle jo heti alun suunnitteluvaiheessa. Tämä lisää järjestelmän kustannuksia, sillä korkean tietoturvatason järjestelmän suunnittelu, toteutus ja operointi vaatii merkittävästi enemmän resursseja ja henkilöstön osaamistason pitää olla korkeammalla tasolla, joten resurssien hintatasokin on korkeampi.

Pilotoinnit kannattaa aloittaa ensin äänestyksillä, jotka eivät ole suoraan minkään lainsäädännön tiukasti säätelemät. Koska osaltaan on ajateltu nettiäänestysjärjestelmän mahdollistavan myös yhdistysten ja järjestöjen äänestämisen, voidaan nettiäänestysjärjestelmää pilotoida helposti erilaisten järjestöjen vaalitapahtumilla. Näissä voidaan alussa pilotoida vain osia järjestelmän toiminnallisuudesta (esimerkiksi tunnistautuminen voi olla kevennetty käyttäjätunnus + PIN-numero) ja siten saada nettiäänestysjärjestelmän eri osien toiminnallisuudesta ja operoitavuudesta merkittävissä määrin tietoa ennen varsinaisen lopullisen järjestelmän toteuttamista ja käyttöönottoa.

Neuvoa-antavien kunnallisten kansanäänestysten nettiäänestysjärjestelmää voidaan siis käyttöönottaa ja pilotoida askeleittain, jos huomioidaan erilaisten järjestöjen ja yhdistysten mahdollinen apu. Jos valtio tarjoaa järjestelmän erilaisten järjestöjen käyttöön testivaiheessa ilman korvausta, on odotettavissa useiden yhdistysten lähtevän mukaan kokeiluun, vaikka järjestelmä tarjoaisi vasta osan lopullisesta toiminnallisuudesta.

Yleisten vaalien vaatimukset nettiäänestysjärjestelmälle ovat korkeammat kuin kunnallisten kansanäänestysten nettiäänestysjärjestelmälle. Jo vaalien prosessitapa on erilainen ja siten ei

järjestöjen ja yhdistysten vaaleista saada välttämättä tarvittavaa lisätietoa yleisten vaalien nettiäänestysjärjestelmän toteuttamiseen. Nettiäänestysjärjestelmä yleisiin vaaleihin pitäisi olla luotettava ja siten sen testaus ja nimenomaan kuormankestävyyden testaaminen on tärkeää. Ei ole järkevää ottaa käyttöön nettiäänestysjärjestelmää, joka ei kykene palvelemaan kaikkia äänestäjiä vaalien aikana. Yleisten vaalien nettiäänestysjärjestelmän testaaminen on merkittävä ponnistus, joka vaatii ison määrän resursseja. Tämä pitää huomioida, jos yleisten vaalien nettiäänestysjärjestelmää joskus otetaan käyttöön.

Yhteenveto

Yhteenvetona esiselvityksestä nousevat esiin seuraavat huomiot:

- Neuvoa-antavan kunnallisen kansanäänestyksen nettiäänestysjärjestelmä on yksinkertaisimmillaan melko kevyt, jolloin järjestelmän hankinta on kannattavaa. Kevyelläkin järjestelmällä saadaan kerättyä varsinaisia vaaleja tukevaa järjestelmää varten merkittävää käyttötietoa järjestelmästä ja äänestäjistä, joka tarkentaisi vaatimuksia varsinaisia vaaleja tukevalle järjestelmälle.
- Neuvoa-antavaa kansanäänestystä ja yleisiä vaaleja ei näillä näkymin kannata toteuttaa samalla järjestelmällä. Tarvittavat järjestelmät ovat luonteiltaan ja erityisesti tietoturvavaatimuksiltaan kovin erilaiset.
- Kansanäänestysjärjestelmä voidaan ja on syytäkin ottaa vaiheittain käyttöön.
- *Varsinaisia vaaleja tukeva järjestelmä on todennäköisesti kallis hankkia. Nykytiedon valossa yleiset vaalit ovat vaikeat järjestää nettiäänestyksenä millään järjestelmällä.*
- Mikäli nettiäänestys on käytössä myös äänestyspäivänä, nettiäänestyksessä mahdollisesti tapahtuvia tietoturvaongelmia tai teknisiä epäselvyyksiä ei voi korvata mitätöimällä nettiäänestystä ja määräämällä vain äänestyspaikassa annettuja ääniä päteviksi. Tämä vähentää merkittävästi järjestelmän luotettavuutta ja mahdollisuutta toipua virheistä ja ulkopuolisten tahojen hyökkäyksistä. Tästä syystä ei suositella nettiäänestyksen käyttämistä äänestyspäivänä.
- Mikäli hyökkääjä pääsee sopivasti vaihtamaan sovelluksen äänestäjän päätelaitteella, hän voi väärentää äänestäjän äänen. Tämän hyökkäyksen mahdollisuuden poistaminen on erittäin vaikeata. *Vaalijärjestelmässä tämän uhan torjuminen on olennaisen tärkeää ja valitettavasti myös kallista.*

Liite 1: Työpajoihin osallistuneet

Työpajojen sisältöön ovat antaneet eri tavoin panoksensa:

Nettiäänestystyöryhmä

Puheenjohtaja:

Johtaja Kirsi Pimiä, oikeusministeriö

Varapuheenjohtaja:

Erityisasiantuntija Olli-Pekka Rissanen, valtiovarainministeriö

Jäsenet:

Neuvotteleva virkamies Markku Mölläri, valtiovarainministeriö

Neuvotteleva virkamies Jussi Aaltonen, oikeusministeriö

Ylitarkastaja Jukka Leino, oikeusrekisterikeskus

Tutkimuspäällikkö Marianne Pekola-Sjöblom, Suomen Kuntaliitto

Professori Kaisa Nyberg, Aalto-yliopisto

Professori Valtteri Niemi Turun yliopisto

Johtaja Sami Borg, Tampereen yliopisto

Antti Vähä-Sipilä, Electronic Frontier Finland EFFI ry

Pysyvä asiantuntija:

Tietopalvelupäällikkö Timo Salovaara, Väestörekisterikeskus

Sihteerit

Ylitarkastaja Heini Huotarinen, oikeusministeriö

Sovellussuunnittelija Marita Kolehmainen, oikeusrekisterikeskus

Kuntien edustajat:

kaupunginlakimies ja keskusvaalilautakunnan sihteeri Lena Filipsson-Korento, Kauniaisten kaupunki

It-asiantuntija Markus Hirvikoski, Helsingin kaupunki

Järjestelmäpäällikkö Jukka Mäntylä, Helsingin kaupunki

Keskusvaalilautakunnan sihteeri Veera Reuna, Helsingin kaupunki

lakimies ja keskusvaalilautakunnan sihteeri Ville Vitikka, Rovaniemen kaupunki

Muut esiselvitykseen nimetyt tahot:

Riskienhallinnan erityisasiantuntija Matti Aitta, oikeusministeriö

Ohjelmakoordinaattori Ira Alanko, valtiovarainministeriö

Tietohallintojohtaja Max Hamberg, oikeusministeriö
Erityisasiantuntija Jari Jauhiainen, oikeusministeriö
Riskienhallintapäällikkö Kimmo Janhunen, Oikeusrekisterikeskus
Vaalijohtaja Arto Jääskeläinen, oikeusministeriö
Erityisasiantuntija Laura Nurminen, oikeusministeriö
Palvelupäällikkö Pauli Pekkanen, Väestörekisterikeskus

Codenton konsultit:
Kaj Mustikkamäki
Lea Viljanen
Matti Kinnunen