Tietoturva-arviointi

HYY:n sähköinen vaalijärjestelmä

Pekka Viitasalo (https://fi.linkedin.com/in/pekkaviitasalo)
Matti Suominen (https://fi.linkedin.com/in/mattisuominen)

Versio	Päivämäärä	Tekijä	Kommentti
0.2	2016-06-17	Pekka Viitasalo, Matti Suominen	Ensimmäinen luonnosversio
0.9	2016-06-20	Pekka Viitasalo, Matti Suominen	HYY:n palautteen mukaiset korjaukset
1.0	2016-06-20	Pekka Viitasalo, Matti Suominen	Sisäinen laadunvalvonta

Sisällysluettelo

1 Johdanto

HYY on järjestämässä syksyn 2016 edustajistovaaleja sähköisesti. Edustajisto on hyväksynyt 25.2.2016 vaalijärjestyksen, jonka mukaan sähköinen äänestys voidaan toimittaa, jos vaalijärjestyksessä esitetyt vaatimukset vaalijärjestelmälle toteutuvat ja tämän on vahvistanut riippumaton auditoija.

HYY on järjestänyt loppuvuodesta 2015 hallintovaalit sähköisesti. HYY:n suunnitelmana on ollut käyttää hallintovaalien vaalijärjestelmää pohjana ja jalostaa siitä edustajistovaaleja varten sähköinen vaalijärjestelmä. Varsinainen vaalijärjestelmän toteutus on tarkoitus tehdä syksyllä 2016.

HYY:n auditointisuunnitelman mukaan auditointi tehdään kahdessa vaiheessa:

1. Keväällä/kesällä 2016 tehtävässä auditoinnissa varmistutaan siitä, että olemassa olevan kaltaisella vaalijärjestelmällä voidaan toteuttaa sähköiset vaalit HYY:n vaalijärjestyksen mukaisesti, kun tunnetut puutteet on korjattu
2. Syksyllä 2016 tehtävässä auditoinnissa varmistutaan siitä, että toteutettu järjestelmä täyttää HYY:n vaalijärjestyksen vaatimukset

Auditoinnin ensimmäistä vaihetta varten toimitettu materiaali sisälsi seuraavan materiaalin:

1. HYY:n vaalijärjestys, jonka edustajisto on hyväksynyt 25.2.2016
2. Edustajistolle laadittu selvitys sähköisestä äänestyksestä; laatinut Petrus Repo ja päivätty 13.3.2015
3. Linkit hallintovaalien äänestysjärjestelmän koodiin

Auditoinnin ensimmäisen vaiheen aloituspalaverissa todettiin seuraavaa:

- Niitä HYY:n vaalijärjestyksessä esitettyjä vaatimuksia, jotka koskevat vaalijärjestelmän tietoturvallisuutta ei ole asetettu niin, että ne olisivat mitattavissa
- Hallintovaaleissa käytetty ohjelmisto ei juurikaan vastaa edustajistovaaleihin suunniteltua ohjelmistoa mm. äänestäjien todennuksen, äänten teknisen tallennuksen ja laskentaosion osilta.

Edellä olevan johdosta aloituspalaverissa sovittiin, että Nixu analysoi vaalijärjestelmälle asetetut vaatimukset, esittää niille mittaustapoja, arvioi miten nykyisen kaltainen ratkaisu sijoittuisi mittareille sekä laatii kehitysehdotuksia tietoturvan parantamiseksi HYY:n vaalibudjetin puitteissa.

Tämä dokumentti on edellisessä kappaleessa kuvattu raportti.

2 Vaatimusten arviointi

Tässä kappaleessa käydään läpi HYY:n vaalijärjestyksessä oleva vaatimukset sähköiselle vaalijärjestelmälle sekä arvioidaan näiden vaatimusten mitattavuutta. Teknisten yksityiskohtien tueksi käytetään uurnavaalianalogioita, joiden avulla on helpompi arvioida vaatimuksen merkittävyyttä.

2.1 Tietoturva ja toimintavarmuus

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Järjestelmän on oltava tietoturvaltaan ja toimintavarmuudeltaan riittävä."

Tämä vaatimus pitää sisällään kaksi eri vaatimusta, jotka eivät ole rinnakkaisia eivätkä yhteismitallisia. Vaatimukset arvioidaan alla erikseen

2.1.1 Tietoturva

Tietoturvaan liittyy useita eri komponentteja ja aspekteja. Kokonaisvaltainen tietoturva-arkkitehtuurikehikko SABSA esittelee tietoturvallisuutta 6x6-matriisilla, joista jokainen solu sisältää oman analysointi-, määrittely- ja dokumentointiprojektinsa. Tässä raportissa auditoijien tarkoitus on käsitellä sellaista subjektiivisesti rajattua kokonaisuutta, joka auditoijien näkemyksen ja kokemuksen perusteella soveltuu parhaiten HYY:n sähköisen äänestyksen tavoitteisiin.

Nykyaikaiset tietojärjestelmät kuvataan yleensä erilaisina pinoina, joissa pinon eri kerrokset käyttävät alla olevan kerroksen palveluja ja tuottavat palveluja päällä olevalle kerrokselle. Tyypillinen tietojärjestelmäpino muodostuu seuraavista kerroksista:

1. Fyysinen laitteisto
2. Laitteisto-ohjelmistot (firmware)
3. Virtualisointiohjelmisto
4. Virtuaalilaite
5. Virtuaalilaitteen laitteisto-ohjelmisto
6. Käyttöjärjestelmä
7. Varusohjelmisto
8. Sovellus

Yllä oleva pino vastaa ns. pilvipalvelua, jossa sovellusta ajetaan "jossain" sijaitsevalta virtuaalikoneelta. Luottamus tietojärjestelmään vaatii luottamuksen jokaiseen pinon kerrokseen. On huomattava, että mikä tahansa tietoturvaongelma pinon pienempinumeroisessa kerroksessa aiheuttaa sen, ettei mihinkään isompinumeroiseen kerrokseen voida enää luottaa.

Tietojärjestelmällä on tyypillisesti elinkaari, joka koostuu seuraavista elinkaaren vaiheista:

1. Toteutus
2. Asennus
3. Käyttö
4. Muutos
5. Poisto

Kokonaisvaltainen tietoturvallisuus vaatisi tarkastelun ja analysoinnin pinon jokaiselle osalle sen jokaisessa elinkaaren vaiheessa.

Vaalijärjestelmä on tarkoitus toteuttaa kansainvälisen toimijan (Heroku) pilvipalvelussa siten, että palvelut ja tiedot sijaitsevat pelkästään EU-alueella. Aluerajaus on tärkeä, koska äänestäjäluettelosta tullaan siirtämään kopio järjestelmään.

Pilvipalvelun tarjoaja tuottaa edellä kuvatusta tietojärjestelmäpinosta kaikki muut osat paitsi sovelluksen (kyseessä on ns. Platform as a Service, PaaS).

Verrattuna uurnavaaleihin, ratkaisu tarkoittaa suunnilleen sitä, että HYY hankkisi vaaliuurnaksi tunnetulta vaaliuurnien toimittajalta mustan laatikon, jossa on äänestyslippujen pudotusta varten aukko päällä ja pohjassa kannellinen aukko, josta äänet saa ulos. Kummastakaan aukosta ei koskaan voisi katsoa laatikon sisälle eikä koskaan voisi tarkastaa miten laatikkoon pudotetut äänet siirtyvät laatikon pohjalle laskentaa varten.

Vaikka ratkaisu kuulostaa vähän hähmäiseltä, auditoijien suositus on hyväksyä tämä. Perusteena on uurnavaalianalogia, jonka mukaan toimittaja toimittaa miljoonia mustia vaaliuurnalaatikoita, julkaisee miten se vaaliuurnansa tekee ja miten vaaliuurnat toimivat. Lisäksi mikään vaaliuurnan aikaisempi käyttäjä ei ole valittanut vaaliuurnien toiminnasta.

Keskusvaalilautakunnan tulee tehdä päätös, täyttääkö Heroku-pilvipalvelun EU:ssa sijaitseva PaaS-palvelu riittävän turvallisuuden määritelmän. Auditoijien näkemys on se, että turvallisuus on riittävä HYY:n edustajistovaaleja varten.

Sovelluksen osalta on tärkeää, että tietoturvallisuus otetaan huomioon läpi sovelluksen elinkaaren. Sovelluksen osalta tietoturvauhat jakautuvat kahteen kategoriaan:

- sovellukseen laaditut takaportit tai muut piilotoiminnallisuudet
- sovellushaavoittuvuudet

Riippumatta turvatoimista, sovelluksessa voi olla aina sovellushaavoittuvuuksia, jotka vain hyökkääjä löytää eli ns. nollapäivähaavoittuvuuksia. Tahattomien sovellushaavoittuvuuksien määrää voidaan vähentää käyttämällä läpi sovelluksen elinkaaren turvallisen ohjelmistokehityksen menetelmiä. Turvallisen ohjelmistokehityksen menetelmiä ovat mm. OWASP OpenSAMM ja Microsoft SDL. Edellä esitetyt kehikot keskittyvät kuitenkin suurelta osin kehitysorganisaation toimintaan; tämän kaltaisessa ohjelmistoprojektissa yleensä riittää, että kehyksistä otetaan käyttöön oleelliset ja hyödylliset osat. Tärkeintä on, että kehitysprosessi on dokumentoitu ja siihen on sisällytetty tietoturvan huomiointi läpi koko kehitysprosessin. **Auditoijien suositus on, että keskusvaalilautakunta edellyttää sovelluksen kehittämistä jonkin dokumentoidun turvallisen ohjelmistokehityksen menetelmän mukaan.**

Asennus- ja muutosvaiheissa on mahdollista joko tuottamuksellisesti tai vahingossa muokata vaalijärjestelmää sellaiseksi, ettei se enää toimi luotettavasti. Riskien minimoimiseksi näiden vaiheiden toiminnot tulee dokumentoida etukäteen tarkasti. Tämä edellyttää kirjallista asennusprosessin kuvausta ja tarkkaa asennussuunnitelmaa sekä kirjallista muutoksenhallintaprosessin kuvausta ja tarkkaa muutossuunnitelmaa.

Vaalijärjestelmän poistovaiheessa tulee varmistua siitä, että vaalisalaisuuden rikkomisen mahdollistava materiaali hävitetään sekä poistettavasta järjestelmästä että varmistuksista. Tämä edellyttää kirjallista poistoprosessin kuvausta sekä tarkkaa poistosuunnitelmaa.

Auditoijien suositus on, että keskusvaalilautakunta edellyttää kirjallisia kuvauksia jokaisesta järjestelmän elinkaaren vaiheesta.

Sovellushaavoittuvuuksien minimoiminen edellyttää turvallista ohjelmistokehitysprosessia. Sovelluksiin saattaa kaikesta huolimatta jäädä kuitenkin sellaisia haavoittuvuuksia, joita

hyökkääjän on mahdollista hyödyntää joko vaalisalaisuuden murtamiseksi tai vaalien tulosten manipuloimiseksi. Teknisellä tietoturvatarkastuksella pyritään varmistamaan, ettei sovelluksessa ole hyödynnettävissä olevia haavoittuvuuksia. HYY:n vaalijärjestys edellyttää sähköiselle vaalijärjestelmälle teknistä tietoturvatarkastusta.

2.1.2 Toimintavarmuus

Toimintavarmuuteen liittyy useita erilaisia tekijöitä. Vaalijärjestelmän kannalta auditoijien mielestä oleellisimmat ovat:

- järjestelmän tulee olla äänestysaikana äänestäjän käytettävissä
- järjestelmän tulee olla käytettävissä, kun äänet lasketaan
- järjestelmän tulee kirjata kaikki annetut äänet
- järjestelmän tulee kirjata äänet oikein
- järjestelmän tulee laskea äänet oikein

Uurnavaaleissa ei saavuteta täydellistä toimintavarmuutta, koska äänten laskennassa sattuu pieniä virheitä. Nämä virheet ovat kuitenkin satunnaisia ja tarkistuslaskennalla virheiden määrä vielä pienenee. Uurnavaalien epätäydellisyys tältä osin on kuitenkin yleisesti hyväksyttyä, koska järjestelmää ei voida parantaakaan.

Uurnavaaleissa kaikkia annettuja ääniä ei välttämättä kirjata oikein, koska osa äänistä hylätään, vaikka äänestäjä olisikin tarkoittanut äänensä jollekin ehdokkaalle. Tämäkin on yleisesti hyväksyttyä, koska järjestelmää ei voida tältäkään osin parantaa.

Muut vaatimukset uurnavaalit toteuttavat edellyttäen, että vaalijärjestäjät ovat varanneet riittävät resurssit äänestyspaikoille sekä ääntenlaskentaan.

Sähköisissä vaaleissa järjestelmän saatavuutta äänestäjien käyttöön äänestysaikana voidaan mitata käytettävyysprosentilla joka on järjestelmän käytettävyysajan suhde koko äänestysaikaan. Lyhyet käyttökatkokset järjestelmässä eivät estä äänestämistä eivätkä sotke vaaleja. Käyttökatkokset voivat kuitenkin tehdä äänestyskokemuksesta sekä hankalan että epämiellyttävän.

Keskusvaalilautakunnan tulee määritellä järjestelmän käytettävyysprosenttitavoite (tai käytettävyysprosenttivaatimus) sekä mitata miten tavoite/vaatimus toteutuu. Auditoijien mielestä vaatimus tulee olla suuruusluokaltaan sellainen, että järjestelmässä voi olla korkeintaan muutama muutaman minuutin käyttökatko. Pidempien katkojen tulisi vaikuttaa mahdollisuuksien mukaan äänestyksen aikaikkunaan.

Äänestysajan päättymisen jälkeen tuloslaskennalle on tiukka aikaikkuna joten järjestelmän tulee olla käytettävissä siten, että äänet voidaan laskea tulostenlaskenta-ajan puitteissa. Tämä mittari on selkeästi binäärinen: joko tavoite toteutuu tai sitten ei.

Keskusvaalilautakunnan tulee määritellä laskenta-ajan pituus ja vaatia, että järjestelmä pystyy toteuttamaan äänten laskennan määritellyn ajan puitteissa.

Vaatimus siitä, että kaikki annetut äänet kirjataan oikein sisältää kaksi vaatimusta: tietojärjestelmän on kirjattava annetut äänet oikein ja äänestäjän on oltava tietoinen siitä, että annettu ääni on kirjattu.

Äänestyksen tulee olla äänestäjän kannalta transaktio, joka joko onnistuu kokonaisuudessaan tai sitten koko toiminto perutaan. Äänestäjälle tulee tulla palaute äänestystapahtumasta, joka kertoo, että ääni on annettu ja kirjattu. Mikäli äänestäjälle tällaista palautetta ei tule, äänestäjän tulee äänestää uudestaan.

Tietojärjestelmän kannalta äänen kirjaaminen on myös transaktio, joka joko onnistuu tai epäonnistuu kokonaisuudessaan. Toteutuksen on tuettava tätä sekä palautetta äänestäjälle äänestyksen onnistumisesta.

Tämä mittari on selkeästi binäärinen: joko tavoite toteutuu tai sitten ei.

Sähköisessä vaalissa äänestäjä voi valita pelkästään annetuista vaihtoehdoista (joista yhden tulee olla tyhjä ääni). Äänestäjä ei voi piirtää äänestyslippuun eikä äänestyslipun lukemisessa tule esim. 1-vai-7-ongelmaa. Asianmukaisesti toimiva tietojärjestelmä kirjaa äänen aina oikein; mittari on puhtaasti binäärinen.

Keskusvaalilautakunnan tulee vaatia, että käyttäjälle annetaan selkeä palaute siitä, että ääni on kirjattu ja ääni tulee kirjata sellaisena kuin äänestäjä sen antoi.

Sähköiseen vaalijärjestelmään kirjatut äänet eivät ole koskaan tulkinnanvaraisia. Koska äänet on tallennettu tietokoneelle sopivassa esitysmuodossa, äänten laskeminen on algoritminen toimenpide ja tulos on deterministinen.

Vaalijärjestelmä voi laskea sähköisen äänestyksen osalta pelkästään ehdokkaiden saamat äänet. Mikäli tämä on tavoite, laskennan tulos täytyy toimittaa järjestelmälle, joka laskee varsinaisen vaalituloksen. Tällöin täytyy kuitenkin tehdä tarkka määrittely siitä missä muodossa laskentatulos esitetään, jotta vaalituloksen laskeva ohjelmisto voi käyttää sitä syötteenään.

Mikäli vaalitapa on pelkästään sähköinen, vaalituloksen laskenta voidaan tehdä äänten laskennan yhteydessä. Tällöin tulee määritellä miten vaalitulos lasketaan, jotta vaalijärjestykseen kirjattu suhteellinen vaalitapa toteutuu.

Keskuslautakunnan tulee määritellä mitä sähköinen vaalijärjestelmä laskee ja miten sekä miten vaalijärjestelmän laskemat tulokset esitetään ja miten ne mahdollisesti viedään vaalituloksen laskentaprosessiin. Mikäli vaalijärjestelmä laskee vaalituloksen, pitää vaatimuksissa esittää miten vaalitulos lasketaan.

2.2 Tiedonsiirron tietoturva

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Äänestäjän äänestyslaitteen ja vaalijärjestelmään liittyvän palvelun välillä on käytettävä riittävää tietoturvaa"

Parhaiden käytäntöjen mukaan tämä saavutetaan käyttämällä ratkaisua, jossa äänestäjä voi varmistua kommunikoivansa vaalijärjestelmän kanssa ja jossa tietoliikenne on suojattu siirrettävän tiedon muokkaukselta ja salakuuntelulta.

Mitattavia ja arvioitavia kohtia ratkaisussa on vaalijärjestelmän todennuksen luotettavuus sekä salauksen ja eheydenvarmistuksen vahvuus. Teknisesti vahvuutta mitataan avainpituudella; parhaiden käytäntöjen mukaiset vahvuudet riittävät nykytilannetta varten.

Uhkaskenaariona on kuitenkin liikenteen tallentaminen ja salauksen purkaminen myöhemmin, kun laskentatehot riittävät. On huomattava, että jokin valtiollinen taho todennäköisesti tallentaa kaiken liikenteen, joka menee vaalijärjestelmään. Merkittävin skenaario on kvanttitietokoneen tulo n. 2030; kvanttitietokoneen avulla nykyiset salausjärjestelmät voidaan purkaa.

Keskusvaalilautakunnan on määriteltävä tavoiteaika, jonka salausratkaisun on suojattava tietoliikennettä. Mikäli tavoitteena on suojaus, joka kattaa yli vuoden 2030, salausratkaisu tulee toteuttaa ns. Post Quantum Cryptography -ratkaisulla, jonka toteuttaminen voi olla erittäin hankalaa.

Äänestäjä todentaa vaalijärjestelmän Internet-maailmassa varmenteella, joka on palvelimen sähköinen henkilöllisyystodistus. Varmenteita voi myöntää moni taho; teknisesti varmenteet ovat samanlaisia mutta semanttinen ero on suunnilleen sama kuin passilla ja itse kirjoitetulla henkilöllisyystodistuksella. Internet-maailmassa on joukko varmenteita myöntäviä tahoja, joita voidaan pitää verrannollisena passin myöntäviin tahoihin; nämä tahot tunnistaa siitä, että niiden ns. luottamusankkurit ovat kaikissa merkittävissä selaimissa.

Keskusvaalilautakunnan tulee määritellä siihen minkälaiselta taholta voidaan vaalijärjestelmän palvelinvarmenne hankkia. Auditoijien suositus on se, että palvelinvarmenne tulee olla sellaiselta taholta, jonka kaikki merkittävimmät selaimet (Google Chrome, Microsoft Internet Explorer, Microsoft Edge, Firefox, Opera, Safari) hyväksyvät luotetuksi. On huomattava, että väärältä taholta tai väärällä sisällöllä oleva palvelinvarmenne johtaa siihen, että käyttäjälle tulee tietoturvavaroitus selaimesta.

2.3 Äänestäjän tunnistaminen

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Äänestäjän henkilöllisyys on tunnistettava ennen äänestämistä."

Tietoteknisesti henkilöllisyyden tunnistamisessa on kysymys todennuksesta eli miten äänestäjä pystyy näyttämään toteen kukan hän on. Uurnavaaleissa äänestäjä näyttää todistuksen henkilöllisyydestään; normaalisti kelvolliset todistukset on rajattu pieneen joukkoon esim. ajokortti, passi, poliisiviranomaisen myöntämä henkilökortti, opiskelijakortti jne.

Sähköisessä vaalissa käyttäjä väittää olevansa joku, jonka jälkeen väite vahvistetaan jollakin tavalla eli tehdään todennus. Todennukseen voidaan käyttää jotain mitä käyttäjä tietää (esim. salasana), jotain mitä käyttäjällä on hallussaan (esim. salasanalista) tai jotain mitä käyttäjä on eli biometria (sormenjälki, retina, iris, kasvotunnistus, ääni jne.). Todennusta sanotaan vahvaksi[1], jos todennukseen vaaditaan edellisestä kolmesta vähintään kaksi tekijää. Heikkoon todennukseen riittää yksi tekijä.

Keskusvaalilautakunnan tulee määritellä vaaditaanko vahva vai heikko todennus.

Suunnitteilla oleva vaalijärjestelmän integraatio yliopistoissa ja korkeakouluissa käytettyyn Haka-ratkaisuun mahdollistaa toistaiseksi pelkästään heikon todennuksen salasanalla.

2.4 Ehdokaslistan esittäminen

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Sähköiseen järjestelmään kirjautumisen jälkeen tulee selkeästi olla näkyvissä ehdokasyhdistelmät."

Tämä vaalijärjestyksen vaatimus ei ole tietoturvavaatimusten piirissä.

2.5 Mahdollisuus äänestää tyhjää

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Äänestäjällä on oltava mahdollisuus äänestää tyhjää."

Tämä vaalijärjestyksen vaatimus ei ole tietoturvavaatimusten piirissä. On huomattava kuitenkin, että myös tämä käyttötapaus kuuluu vaalisalaisuuden piiriin.

[1] VAHTI 12/2006: Tunnistaminen julkishallinnon verkkopalveluissa, https://www.vahtiohje.fi/web/guest/kayttajien-tunnistaminen-verkkopalveluissa

2.6 Vaalisalaisuus

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Äänestäjän henkilöllisyys ei saa olla yhdistettävissä mihinkään tiettyyn annettuun ääneen."

Uurnavaaleissa vaalisalaisuus perustuu siihen, että äänestysliput ovat anonyymejä ja niitä on uurnassa useita. Vaalisalaisuus voisi vaarantua, jos äänestyslippuja olisi erittäin vähän uurnassa tai ääntenlaskija tunnistaisi äänestäjän käsialan. Asianmukaisesti järjestetyissä vaaleissa kummatkin mahdollisuudet ovat niin pieniä, että niitä pidetään hyväksyttyinä riskeinä.

Sähköisessä vaalissa käyttäjä tunnistetaan ja tunnistustieto viedään vaalijärjestelmälle samalla kun käyttäjä antaa äänensä. Tämä vaaditaan, jotta voidaan luoda kokonaistransaktio, jossa varmistetaan sekä se, että äänioikeutta käytetään tasan yhden äänen verran, että tämä ääni vastaa käyttäjän äänestystahtoa.

Mikäli äänestäjän valinta toimitetaan vaalijärjestelmälle siten, ettei sitä ole vaalijärjestelmän käsittelyä varten salattu, äänestystapahtuman elinkaaren alkupäässä äänestäjän valinta on yhdistettävissä äänestäjään. Jos tältä halutaan välttyä, pitää äänestäjällä olla käytettävissä järjestelmä, jolla ääni salataan ennen sen toimittamista äänestysjärjestelmälle. Teknisestä salaus olisi tehtävissä joko puhelinsovelluksella tai selaimella joten vaativia erityisjärjestelyjä ei tarvittaisi.

Keskusvaalilautakunnan on määriteltävä pitääkö äänen salaus tehdä käyttäjän päätelaitteella ennen kuin ääni siirretään vaalijärjestelmään.

Mikäli käyttäjälle halutaan antaa mahdollisuus useaan äänestyskertaan, esimerkiksi painostettuna annetun äänen kumoamiseen, pitää ääni ja äänestäjä linkittää toisiinsa vaalijärjestelmässä koko äänestysajan. Jos ääni on salaamaton, vaalijärjestelmän ylläpitäjällä on mahdollisuus katsoa kaikkien äänestäjien äänet.

Mikäli käyttäjälle ei haluta antaa mahdollisuutta useaan äänestyskertaan, äänen linkitys äänestäjään voidaan poistaa osana äänestystapahtumaa. Tällöin vaalijärjestelmään kirjataan tieto siitä, että äänestäjä on käyttänyt äänioikeutensa ja ääni kirjataan sähköiseen uurnaan anonyymisti. Tällöin äänen salaamattomuudella ei ole merkitystä enää itse äänestystapahtuman jälkeen.

Keskusvaalilautakunnan on määriteltävä onko äänestäjällä mahdollisuus äänestää useita kertoja siten, että viimeisin ääni jää voimaan.

Mikäli aikaisemmat päätökset ovat sellaiset, ettei ääntä salata käyttäjän päätelaitteella ja äänestäjä voi äänestää useita kertoja, keskusvaalilautakunnan on päätettävä pitääkö äänet salata vaalijärjestelmässä ennen äänten tallennusta. Päätös ottaa kantaa siihen onko ylläpitäjällä mahdollisuus nähdä koko äänestysajan kuka äänesti ketä.

Mikäli salaus otetaan käyttöön, tyypillinen toteutus on ns. julkisen avaimen salaus. Salaus toimii siten, että käytössä on avainpari, jossa on julkinen komponentti, jolla voidaan salata, sekä salainen komponentti, jolla salaus voidaan purkaa. Jossain vaiheessa äänten salaus pitää purkaa, jotta äänet voidaan laskea. Tyypillisesti avain, jolla salaus voidaan purkaa, on usean henkilön kontrollissa eli yksi yksittäinen henkilö ei voi tehdä salauksen purkua. Usean henkilön kontrolli voidaan toteuttaa teknisenä pakkona. Uurnavaaleissa käytäntönä HYY:llä on se, että kaikki äänestyksen kannalta kriittiset toimet vaativat vähintään kolmen henkilön osallistumisen.

Mikäli äänet päätetään salata, keskusvaalilautakunnan pitää määritellä montako henkilöä vaaditaan paikalle, jotta salaus voidaan purkaa ääntenlaskua varten.

2.7 Äänioikeuden rajoitus

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Äänestäjä voi käyttää äänioikeuttaan vain kerran."

Uurnavaaleissa käytössä on lista äänioikeutetuista, johon tehdään merkintä, kun äänestäjä tulee käyttämään äänioikeuttaan. Vastaavasti sähköisessä vaalijärjestelmässä on lista äänioikeutetuista, johon tulee tehdä merkintä, kun äänioikeutta on käytetty.

Tietyillä toteutustavoilla sähköisessä vaalijärjestelmässä vaatimuksen voi toteuttaa siten, että äänestäjä voi tehdä useita äänestystapahtumia, joissa hän antaa äänensä, mutta näistä vain yksi tapahtuma jää voimaan; tyypillisesti tapahtuma on viimeisin. Edellisessä, vaalisalaisuutta käsittelevässä kappaleessa on esitetty, että keskusvaalilautakunnan tulee ottaa kantaa siihen voiko äänestäjä äänestää useita kertoja mutta käyttää kuitenkin äänioikeuttaan vain kerran.

2.8 Avoin lähdekoodi

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Vaalijärjestelmä perustuu avoimeen lähdekoodiin."

Tämä vaalijärjestyksen vaatimus ei ole tietoturvavaatimusten piirissä.

2.9 Järjestelmän pääsyoikeudet

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Keskusvaalilautakunta hyväksyy selosteen järjestelmän pääsyoikeustasoista."

Sähköistä vaalijärjestelmää varten pitää määritellä järjestelmälle vähintäänkin pääkäyttäjätunnus, jolla on käytännössä kaikki oikeudet järjestelmään. **HYY:n vaalibudjetin mukaisissa toteutuksissa pääkäyttäjällä on mahdollisuus muokata vaalitulosta vapaasti jäämättä siitä kiinni.** Jos ääniä ei ole salattu äänestäjän päätelaitteella, pääkäyttäjätunnuksella on mahdollista myös rikkoa vaalisalaisuus; toteutuksesta riippuen joko läpi vaalien tai yksittäisten äänestystapahtumien alkuvaiheessa.

Vaalijärjestelmässä voi olla myös alemman tason käyttäjiä. Näillä käyttäjillä voi olla esim. oikeudet päivittää äänestäjäluetteloa tai ehdokaslistoja.

Pääkäyttäjäoikeus voidaan toteuttaa teknisesti siten, että toimiin vaaditaan usean henkilön läsnäolo. **Keskusvaalilautakunnan tulee määritellä montako henkilöä vaaditaan paikalle, jotta järjestelmään voidaan kirjautua pääkäyttäjänä tai sellaisena käyttäjänä, jolla on mahdollista manipuloida vaalitulosta tai rikkoa vaalisalaisuutta.**

3 Vaalijärjestelmän arviointi

Vaalijärjestelmästä ei ole vielä edustajistovaaliin sopivaa versiota. Arvioitava järjestelmä on hybridi, joka koostuu hallintovaalijärjestelmästä sekä muutossuunnitelmista. Koska järjestelmää ei toistaiseksi ole olemassa, tämä arviointi suurelta osalta spekulatiivinen.

3.1 Toimintavarmuus ja tietoturva

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Järjestelmän on oltava tietoturvaltaan ja toimintavarmuudeltaan riittävä."

Vaalijärjestelmää ei voida arvioida tältä osin tässä vaiheessa, koska sekä toteutus on kesken että vaatimuksia ei ole vielä määritelty täsmällisesti.

3.2 Tiedonsiirron tietoturva

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Äänestäjän äänestyslaitteen ja vaalijärjestelmään liittyvän palvelun välillä on käytettävä riittävää tietoturvaa"

Vaalijärjestelmälle ei ole asennettu vielä vaaleissa käytettävää palvelinvarmennetta. Käytössä oleva palvelinvarmenne on Heroku-palvelun yleinen palveluvarmenne. Manuaalisen tarkastuksen perusteella yhteys on suojattu tasolla, joka riittää arviolta suunnilleen vuoteen 2030 asti.

3.3 Äänestäjän tunnistaminen

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Äänestäjän henkilöllisyys on tunnistettava ennen äänestämistä."

Edustajistovaaleja varten vaalijärjestelmä on tarkoitus integroida yliopistojen ja korkeakoulujen yhteiseen Haka-järjestelmään. Äänestäjän tunnistaminen ja todentaminen tapahtuu käyttäjätunnuksella ja salasanalla. Kyseessä on ns. heikko todennus. Todennus on kuitenkin riittävä yliopistojen ja korkeakoulujen järjestelmien käyttämiseksi.

3.4 Ehdokaslistan esittäminen

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Sähköiseen järjestelmään kirjautumisen jälkeen tulee selkeästi olla näkyvissä ehdokasyhdistelmät."

Järjestelmän nykyversiosta tätä ei voida arvioida.

3.5 Mahdollisuus äänestää tyhjää

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Äänestäjällä on oltava mahdollisuus äänestää tyhjää."

Järjestelmän nykyversiosta tätä ei voida arvioida.

3.6 Vaalisalaisuus

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Äänestäjän henkilöllisyys ei saa olla yhdistettävissä mihinkään tiettyyn annettuun ääneen."

Vaalijärjestelmän nykyversiossa annettu ääni näkyy tietokannassa siten, että siihen on yhdistetty äänestäjä. Järjestelmän pääkäyttäjäoikeuksilla voidaan sekä katsoa että muuttaa näitä tietoja. Vaalijärjestys ei ota kantaa voiko näin olla.

Nykymallisessa toteutuksessa linkitys on käytännössä välttämätön toiminnan kannalta, koska sitä käytetään esimerkiksi äänen muttamisessa. Tällöin järjestelmän täytyy tietää, mikä ääni järjestelmästä on poistettava ennen kuin uusi ääni voidaan lisätä jotta yksittäiselle henkilölle ei voi muodostua kahta samanaikaista ääntä.

Alustavissa keskusteluissa nostettiin esiin mahdollisuus, että toteuusta oltaisiin muuttamassa tämän toiminnon osalta. Raportin kirjoitushetkellä ei ole vielä selvää, millainen muutos olisi ja kuinka se vaikuttaisi äänten ja henkilöiden yhdistämiseen tai muihin vaatimuksiin.

3.7 Äänioikeuden rajoitus

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Äänestäjä voi käyttää äänioikeuttaan vain kerran."

Vaalijärjestelmän nykyversiossa tämä on toteutettu teknisesti siten, että tietokannassa voi olla vain yksi ääni äänestäjää kohden. Äänestäjällä on mahdollisuus äänestää useita kertoja mutta vain viimeisin ääni jää voimaan.

Olemassaolevassa toteutuksessa tämä vaatimus on ristiriidassa vaalisalaisuuden kanssa. Jotta ääniä voi nykyisessä mallissa muuttaa, äänet täytyy voida yhdistää suoraan äänestäjään. Tilanteen muuttaminen edellyttää muutosta tietokantarakenteessa ja ohjelmiston logiikassa.

3.8 Avoin lähdekoodi

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Vaalijärjestelmä perustuu avoimeen lähdekoodiin."

Vaalijärjestelmän lähdekoodi on GitHub-palvelussa nähtävissä. Avoimen lähdekoodin vaatimus toteutuu.

3.9 Järjestelmän pääsyoikeudet

Vaalijärjestyksessä vaatimus on esitetty seuraavassa muodossa: "Keskusvaalilautakunta hyväksyy selosteen järjestelmän pääsyoikeustasoista."

Vaalijärjestelmälle ei ole toistaiseksi laadittu selostetta pääsyoikeustasoista.

4 Vaalijärjestelmän kehityssuositukset

Nykyisen vaalijärjestelmän ohjelmistokoodi näyttää laadukkaalta ja auditoijien mielestä kehitystä voidaan jatkaa olemassa olevasta koodipohjasta. Kattava analyysi edellyttää kuitenkin vielä erillisen katselmoinnin, jonka on suunniteltu toteutettavaksi tämän tarkastuksen loppuvaiheessa.

Seuraavassa esitetään muutamia vaalijärjestelmän kehityssuosituksia, jotka on mahdollista toteuttaa HYY:n vaalibudjetin puitteissa.

4.1 Usean käyttäjän kontrolli ylläpitotoiminnoissa

Kaikki järjestelmän ylläpitotoiminnot tulee määritellä sellaiseksi, että niihin vaaditaan vähintään kaksi henkilöä. Teknisesti tämä on mahdollista toteuttaa esim. jaetun salasanan avulla.

Uurnavaaleissa HYY:n vaalijärjestys edellyttää kolmea henkilöä kaikkiin sellaisiin toimintoihin, jotka voivat vaikuttaa vaalien turvallisuuteen.

4.2 Järjestelmän tekninen auditointi

Järjestelmässä mahdollisesti olevat tietoturvapuutteet voivat osittain tai täysin estää suunniteltujen kontrollien toiminnan. Tästä johtuen on tärkeää, että kokonaisuudelle tehdään tekninen tietoturvatestaus ennen käyttöönottoa. Tämän tarkastuksen jälkeen järjestelmää ei saa enää muuttaa teknisesti, koska muutoin tarkastuksen tulokset eivät välttämättä kuvaa järjestelmän todellista tilaa.

Järjestelmän käyttöönotossa on tärkeää varmentaa, että palvelimille todellisuudessa asennetaan sama järjestelmä, joka on aikaisemmin todettu turvalliseksi. Asennus on tärkeää tehdä useamman henkilön kesken jotta voidaan varmistua, ettei yksittäinen ylläpitäjä voi asentaa palvelimelle väärää sovellusta. Asennuksen onnistuminen voidaan todentaa esim. vertaamalla eri tiedostojen tiivistesummia alkuperäisen sovelluksen vastaaviin asennuksen jälkeen.

4.3 Prosessien dokumentointi

Kaikki vaalijärjestelmän elinkaareen liittyvät prosessit tulee dokumentoida tarkalla tasolla, jotta jälkikäteen voidaan osoittaa toiminnan olleen huolellista.

Järjestelmän asennuksesta tulee kuvata ainakin:

- Miltä medialta järjestelmä asennetaan ja mistä se saadaan ko. medialle turvallisesti
- Kaikki asennukseen liittyvät komennot yksityiskohtaisesti, jotta asennusta valvovat henkilöt pystyvät seuraamaan asennusta ja tarvittaessa keskeyttämään sen, mikäli asennuksessa tulee poikkeama

Muutoksista pitää dokumentoida ainakin

- muutoksen vaikutusten arviointi
- miten muutos on testattu ja miten testitulokset arvioitu
- miten muutos hyväksytään tuotantoon
- miten palataan vanhaan, jos muutos kaikesta huolimatta rikkoo jotain

5 Yleistä sähköisistä vaalijärjestelmistä

Miksi sähköisten vaalien järjestäminen olisi vaikeaa, koska pankkien välillä voidaan luotettavasti siirtää rahaa ilman ongelmia?

Pankkitoiminta onnistuu, koska kaikista tapahtumista jää tarkat jäljet erilaisiin lokijärjestelmiin. Mikäli joku tapahtuma kiistetään, lokeilta voidaan rekonstruoida mitä on tapahtunut.

Sähköisissä vaaleissa tilanne on täysin toinen. Vaalisalaisuuden takia äänestystapahtumaa ei voida tallentaa siten, että se voitaisiin myöhemmin rekonstruoida. Äänestäjällä ei ole myöskään mahdollisuutta arvioida onko oma ääni otettu huomioon tuloslaskennassa oikein vai ei, koska ääniä on niin paljon ja ne ovat oletetusti kaikki anonyymejä.

Edellä olevista syistä sähköinen vaali perustuu pelkästään luottamukseen ilman mahdollisuutta jälkikäteen tehtävään varmistukseen. Vaaliohjelmiston pitää olla sellainen, että sen toiminta on mahdollista ymmärtää ilman teknistä osaamista. Lisäksi vaaliohjelmiston tulee olla sellainen, että sen voi tarkistaa kuka tahansa, jolla on riittävä tekninen osaaminen.

Virossa on käytössä sähköinen vaalijärjestelmä, joka pohjautuu merkittävästi Virossa käytössä olevaan sähköiseen henkilökorttiin. Lisäksi äänestykseen liittyy vaalikohtainen julkisen avaimen menetelmällä toteutettu salausavain, jonka salauksen purkamiseen pystyvä osa on suojattu salauslaitteella ja jonka käyttö vaatii usean henkilön yhtäaikaisen läsnäolon.

Viron vaalijärjestelmä toimii kaksivaiheisesti. Ensimmäisessä vaiheessa tehdään äänestys ja toisessa vaiheessa äänet lasketaan. Ensimmäisen vaiheen aikana sähköinen ääni on linkitetty äänestäjään mutta ääni on salattu siten, ettei ääntä voida tulkita. Ääni on allekirjoitettu äänestäjän toimikortilla joten se on suojattu muutosta vastaan.

Äänestyksen päätyttyä alkaa vaalin toinen vaihe. Tallennetut salatut äänet poimitaan tietokannasta siten, että ne irrotetaan linkistä äänestäjään. Äänet tallennetaan DVD-levylle ja levy siirretään laskentajärjestelmälle. Laskentajärjestelmää varten aktivoidaan salauslaite siten, että sitä voidaan käyttää sähköisten äänien tulkitsemiseksi. Salauslaitteen aktivointi vaatii usean henkilön yhtäaikaisen läsnäolon.

Viron vaalijärjestelmää vastaan on esitetty kritiikkiä ja joukko tietoturva-asiantuntijoita on esittänyt, että vaalijärjestelmää voidaan manipuloida[2].

[2] https://jhalderm.com/pub/papers/ivoting-ccs14.pdf