Tietoturva-arviointi

HYY:n sähköinen vaalijärjestelmä

Pekka Viitasalo (https://fi.linkedin.com/in/pekkaviitasalo)
Matti Suominen (https://fi.linkedin.com/in/mattisuominen)
Teo Selenius (https://fi.linkedin.com/in/teo-selenius-0509318b)

Versio	Päivämäärä	Tekijä	Kommentti
0.2	2016-09-23	Pekka Viitasalo, Matti Suominen	Ensimmäinen luonnosversio
0.9	2016-09-24	Pekka Viitasalo, Matti Suominen	HYY:lle lähtevä versio kommentteja varten
1.0	2016-09-26	Pekka Viitasalo, Matti Suominen	HYY:n kommentit huomioitu

Tiivistelmä

HYY on järjestämässä syksyn 2016 edustajistovaaleja sähköisesti. Edustajisto on hyväksynyt vaalijärjestyksen, joka asettaa vaatimukset vaalijärjestelmälle sekä edellyttää, että vaalijärjestelmä auditoidaan.

Vaalijärjestelmän auditointi käynnistyi keväällä 2016 auditoinnin ensimmäisellä vaiheella. Ensimmäisen vaiheen aloituspalaverissa sovittiin, että auditoinnin tekijä, Nixu Oyj, tekee konsultatiivisen arvioinnin vaatimuksille ja esittää niihin kehitysehdotukset, jotta vaatimukset olisivat selvät, ymmärrettävät ja mitattavat.

Keskusvaalilautakunta hyväksyi kokouksessaan 30.6.2016 Nixun esityksen pohjalta vaatimuslistan, jonka vaatimukset sähköisen vaalijärjestelmän tulee toteuttaa. Tämä raportti on tietoturva-arviointi siitä miten HYY:n vaalijärjestelmä nämä vaatimukset toteuttaa.

HYY:n vaalijärjestelmän vaatimukset ovat sellaiset, että ne ovat riittävät ylioppilaskuntavaaleille.

Vaatimukset lähtevät siitä, että järjestelmä toteutetaan Euroopassa sijaitsevaan pilvipalveluun ja lähtökohtaisesti pilvipalvelun toteuttajaan ja ylläpitäjiin luotetaan.

Järjestelmän teknisen tietoturvan tulee olla sellainen, ettei järjestelmän murtamiseen riitä yksittäisen osaavan tietomurtautujan kyvyt.

Toisin kuin monissa julkisuutta saaneissa sähköisissä vaalijärjestelmissä (esim. Viro), tässä järjestelmässä ei ole pyritty toteuttamaan esim. salaukseen perustuvaa teknistä toteutusta, joka pyrkisi varmentamaan äänien oikeellisuuden ja vaalituloksen eheyden. Järjestelmä on teknisesti sellainen, että tulosta olisi mahdollista muuttaa joko manipuloimalla itse järjestelmää tai muuttamalla tulosta suoraan.

Koska ylläpidolla on mahdollisuus sekä muuttaa vaalijärjestelmää että manipuloida vaalitulosta, ratkaisuksi on valittu Dual Control eli kaikkiin ylläpito-operaatioihin tarvitaan kahden fyysisesti samassa tilassa olevan pääkäyttäjän yhteistyö. Järjestelmän tekninen turvattomuus vihamielistä ylläpitoa vastaan hyväksytään riskinä.

Vaalijärjestelmän arvioinnissa tarkastettiin vaalijärjestelmän dokumentaatio, katselmoitiin vaalijärjestelmän ohjelmakoodi sekä tehtiin vaalijärjestelmälle tekninen tietoturvatarkastus.

Tarkastuksen tulos on se, että HYY:n vaalijärjestelmä täyttää sille asetetut vaatimukset.

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 toista vaihetta varten Nixulle toimitettiin

- pääsy vaalijärjestelmän laadunvarmistusympäristöön, joka on tuotannon kaltainen käyttöönoton kannalta mutta sisältää testidataa
- pääsy vaalijärjestelmän lähdekoodiin
- pääsy vaalijärjestelmän dokumentaatioon

Auditoinnin toisessa vaiheessa tarkastettiin, että toteutettu vaalijärjestelmä täyttää ne vaatimukset, jotka Keskusvaalilautakunta kokouksessaan 30.6.2016 hyväksyi.

Tämä dokumentti on auditoinnin toisen vaiheen raportti. Sekä koodikatselmoinnista että teknisestä tietoturvatarkastuksesta on toimitettu yksityiskohtaisempi ja teknisempi raportti järjestelmän kehittäjille.

2 Vaatimusten toteutumisen arviointi

Tässä kappaleessa kuvataan miten tarkastus on tehty ja mitkä ovat tarkastuksen tulokset.

2.1 Aikataulu

Järjestelmän tekniset tarkastukset on tehty aikavälillä 19-23.9.2016. Järjestelmän koodia on käyty läpi useampaan kertaan kehityksen aikana ja jo ennen tarkastusta. Kaikki tämän raportin huomiot koskettavat kuitenkin lopullista versiota, joka on tarkoitus ottaa myös käyttöön varsinaiseen äänestykseen.

2.2 Käytetyt menetelmät

Vaalijärjestelmän turvallisuus pohjautuu sekä tekniseen toteutukseen että järjestelmän käytön ja ylläpidon turvallisiin prosesseihin.

Prosessien turvallisuuden arviointi on tehty pelkästään prosessidokumentaatioon pohjautuen, koska järjestelmä ei ole sellaisenaan ollut vielä käytössä ja siten prosessien toteutumisesta ei ole olemassa minkäänlaista konkreettista aineistoa.

Järjestelmän teknisen toteutuksen tarkastus pohjautuu ohjelmakoodin katselmointiin ja laadunvarmistusympäristön tekniseen tietoturvatestaukseen. Testaus on tehty tuotannon kaltaisessa ympäristössä, jossa käytössä oli todellisen kaltaista testidataa.

Koodikatselmoinnissa on tarkastettu, että

- koodin ulkoasu on selkeä ja luettava
- koodissa ei ole tahallisia takaportteja järjestelmään tai muita sellaisia mekanismeja, jotka selkeästi pyrkisivät vääristämään vaalitulosta
- koodissa ei ole käytetty turvattomia ratkaisuja

Teknisessä tietoturvatestauksessa on käytetty parhaisiin käytäntöihin kuuluvia testaustyökaluja:

- Burp Suite Professional - sekä automaattisia että manuaalisia tarkastuksia
- SSLScan - tietoliikenteen salauksen tarkastus

Järjestelmän luonteesta johtuen testaus on ollut pitkälti manuaalista, koska hyökkäyspintaa on hyvin rajallisesti ja relevantit ongelmat liittyvät pitkälti erilaisiin selkeisiin väärinkäyttötapauksiin.

Järjestelmän alustaa ei erikseen testattu, koska käytössä on vakiotu palvelinalusta, johon ei ylläpidon toimesta voida tehdä muutoksia ja jonka päivitykset sekä mahdolliset tietoturvakovennukset tehdään palveluntarjoajan toimesta.

2.3 Havainnot

Keskusvaalilautakunnan vaatimukset on kirjattu kokouspöytäkirjan liitteeksi. Liitteessä osa vaatimuksista on saatavuuteen ja suorituskykyyn liittyviä vaatimuksia, joita ei tässä arvioinnissa ole testattu ja joita ei tässä raportoida. Seuraavassa jokaiseen yksittäiseen vaatimustaulukkoon on kirjattu liitteen yhden Excel-solun sisältö.

Seuraavassa vaalijärjestelmä viittaa kokonaisuutteen, äänestysjärjestelmä siihen vaalijärjestelmän osaan, jonka kautta äänestys tapahtuu ja laskentajärjestelmä siihen osaan, joka laskee vaalin tulokset äänestysjärjestelmän tallentamista äänistä. Laskentajärjestelmän tallentamat vaalitulokset esitetään tulosjärjestelmällä.

Vaatimus	
Vaaditaan tunnettu toimija ylläpitokumppaniksi, jolla uskottavat prosessit konesalitoiminnassa Data pysyy EU alueella	OK
HYY:n vaalijärjestelmän alustana toimii Heroku-pilvipalvelun Euroopan instanssi. Heroku on perustettu vuonna 2007 ja se kuuluu nykyisin Salesforce-konserniin. Varsinainen vaalitulos tallennetaan Amazon AWS -palveluun. Amazon AWS on yksi maailman suurimmista pilvipalvelujen tarjoajista ja sitä käyttää ja siihen luottaa useat suuryritykset. Vaalitulos on julkinen.	

Vaatimus	
Toteutus käydään läpi tunnettujen haavoittuvuuksien osalta Arkkitehtuuri suunnitellaan parhaiden käytäntöjen mukaiseksi	OK
Arkkitehtuuri erittelee eri toiminnot omiksi kokonaisuuksikseen, joissa kukin osa tekee vain sille määritellyt toimet. Tämä tekee järjestelmän toimivuuden arvioinnin helpommaksi. Ulospäin näkyvä osa järjestelmää on hyvin suppea eikä tarjoa juuri muuta toiminnallisuutta kuin mahdollisuuden äänestää sekä käyttäjän tarvitsemaan tietoa vaaleista. Ratkaisu on hyvä, sillä suurin riski, jolta täytyy teknisesti suojautua, liittyy järjestelmän tahalliseen tai tahattomaan väärinkäyttöön ulkoisen tahon (esim. äänestäjä) toimesta. Nykyinen arkkitehtuuri minimoi riskit tältä osin.	

Vaatimus	
Järjestelmän käytön vaiheet kuvataan suunnittelun yhteydessä	OK
Vaalijärjestelmän elinkaaren hallinta on toteutettu Github-palvelun avulla. Github toimii sekä lähdekoodin että dokumentaation tallennuspaikkana ja ohjelmistokomponentit voidaan hallitusti viedä palvelimille. Dokumentaatio ottaa kantaa siihen, kuinka järjestelmät viedään palvelimille. Suurin osa toimista on automatisoitu niin, että inhimilliset virheet voidaan minimoida.	

Vaatimus	
HAKA-todennuksen toimimattomuuteen on varauduttava	OK
Teknisesti tähän on varauduttu siten, että ylläpitoliittymästä voidaan lisätä äänestäjä. Ratkaisu ei kuitenkaan skaalaudu kattamaan koko jäsenistöä mikäli HAKA-todennus on kokonaan toimimaton.	

Vaatimus	
Järjestelmän tulee kertoa äänestyshetkellä, kenelle ääni on annettu Järjestelmän tulee kertoa äänestyshetkellä, että ääni on kirjattu	OK
Järjestelmästä saa ulos riittävän tiedon visuaalisesti. Mekanismin luotettavuus nojaa siihen, että järjestelmää ei ole muokattu tai muuten manipuloitu toimimaan taustalla eri tavalla kuin mitä käyttöliittymä antaa ymmärtää. Äänestäjällä ei ole teknistä mahdollisuutta varmistaa tätä erikseen, mikä on hyväksytty riski järjestelmän suunnittelussa.	

Vaatimus	
Laskenta tehdään erillisessä järjestelmässä äänestysdatan pohjalta Ehdokkaiden asettelu tehdään erillisessä järjestelmässä Missään järjestelmässä ei saa olla ylimääräistä toiminnallisuutta	OK
Laskennan tulee tapahtua erillisessä järjestelmässä	OK
Äänestysjärjestelmä kirjaa pelkät äänet tietokantaan. Äänestyksen jälkeen vaalityöntekijä voi käynnistää laskentaohjelmiston, joka käyttää automaattisesti äänestysjärjestelmään kirjattuja ääniä. Ehdokkaiden asettelu tehdään erillisen hallintaliittymän kautta. Kaikki järjestelmän eri komponentit ovat käytännössä erillisiä ohjelmia tai komponentteja, joilla on oma rajattu tehtävänsä. Tämän arkkitehtuuriratkaisun kautta koko vaatimus toteutuu.	

Vaatimus	
Järjestelmä varmistaa äänestystietojen eheyden. Järjestelmä raportoi poikkeuksista.	OK
Tietojen eheyttä pyritään varmistamaan teknisessä mielessä tekemällä tarkastusta syötteille ja muuten varmistamaan, että teknisesti tieto kulkeutuu tietokantaan eheänä. Virheistä kirjataan tietoa lokiin, jota voidaan tarvittaessa katsoa jälkikäteen ongelmatilanteissa. Testauksen aikana tunnistettiin useita poikkeustilanteita, joista syntyi todistettavasti merkintä lokiin kun testaaja pyrki väärinkäyttämään järjestelmää. Tältä osin vaatimus toteutuu.	

Vaatimus	
Järjestelmän tulee varmistaa, että tuloksia ei voi manipuloida ennen siirtoa esitysjärjestelmään Ylläpito vaatii samat oikeudet ylläpitäjiltä kuin muissakin vaiheissa kunnes vaalit ovat ohi.	**OK**
Tarkastuksen perusteella vaalijärjestelmä ei manipuloi ääniä minkään tietoisesti toteutetun mekanismin kautta, joka olisi havaittu järjestelmässä. Tietojen muokkaus edellyttäisi ylläpidolta aktiivisia toimia tai hyökkääjän, joka onnistuisi murtautumaan järjestelmään. Nämä erikoistilanteet katetaan muissa vaatimuksissa.	

Vaatimus	
Vaalien läpivienti pyritään automatisoimaan niin, että tiedot siirtyvät ilman manuaalista prosessia	**OK**
Järjestelmässä on toteutettu rajapintoja, joilla eri komponentit voivat kommunikoida toisilleen siinä määrin, kun se on tulosten keräämisen, laskennan ja näyttämisen osalta tarpeellista. Poikkeustilanteissa käytettävä manuaalinen prosessi nojaa samoihin turvakontrolleihin kuin muukin ylläpito.	

Vaatimus	
Vaalituloksen laskenta toteutetaan vaalijärjestyksen määrittämällä tavalla	**OK**
Järjestelmän läpikäynnissä ei havaittu poikkeuksia laskentatavassa, vaikka tämä ei ollutkaan tarkastuksen pääasiallinen kohde. Tulokset on myös mahdollista laskea erikseen uudelleen käsin tietojen pohjalta jos syntyy epäilys, että järjestelmän laskentaa ei ole toteutettu oikein.	

Vaatimus	
Vaalitulos esitetään erillisessä järjestelmässä, johon pätee samat vaatimukset ylläpidosta kuin muihinkin vaalijärjestelmän osiin	OK
Mikäli automaattista laskentaa ei voida toteuttaa, vaaditaan kahden henkilön kontrolli, jotta äänet voidaan siirtää laskentaa varten.	OK
Ylläpitotehtäviin vaaditaan aina kahden henkilön läsnäoloa Rajoitus koskee kaikkia järjestelmän komponentteja, joissa äänestystulosta käsitellään.	OK
Kaksi henkilöä tarvitaan muutoksien tekemiseen Olemassa tieto siitä, mikä versio on auditoitu ja varmistetaan käyttöönoton yhteydessä, että oikea versio laitettiin paikoilleen Muutokset vaalien aikana voidaan hyväksyä kahden henkilön päätöksellä Muutoksista jäätävä kirjaukset (mitä muutettiin ja miksi), kirjaukset tarkastetaan erikseen	OK
Dokumentoidun vaaliprosessin mukaan kaikki ylläpitotoiminta noudattaa Dual Control -periaatetta eli jokaiseen ylläpito-operaatioon tarvitaan kahden pääkäyttäjän fyysinen läsnäolo samassa tilassa. Dokumentoidun vaaliprosessin mukaan vaalien käynnistyksessä tarkastetaan, että vaalijärjestelmän versio on tarkastettu ja hyväksytty versio. Vuoden 2016 vaaleissa versio on auditoitu versio. Dokumentoidun vaaliprosessin mukaan kaikista ylläpitotoiminnoista tehdään pöytäkirja. On tärkeä huomata, että järjestelmän tekninen toteutus ei lähtökohtaisesti tarjoa mekanismeja, joilla voitaisiin suojautua vihamielistä ylläpitäjää vastaan. Järjestelmän eheys, tietojen muuttumattomuus ja muut väärinkäyttötilanteet estetään etupäässä tämän prosessin avulla, ei suoranaisesti teknisillä keinoilla.	

Vaatimus	
Vaalijärjestelmän todennukseen vaaditaan jokin luotettava ja tunnettu varmenne, joka on kaikkien yleisimpien selaimien tukema.	OK
Valittu varmentaja on RapidSSL, joka itse ilmoittaa, että sen varmenteisiin luottaa yli 99% selainversioista.	

Vaatimus	
Järjestelmän tulee kirjata tieto aina, jos tehdään muutoksia järjestelmään ja tietoihin. Järjestelmän tulee kirjata tieto kirjautumisista ylläpitoliittymiin. Ei saa vaarantaa vaalisalaisuutta lokien kautta. Lokien tulee olla sijoitettuna mahdollisuuksien mukaan niin, että ylläpitäjän ei ole niitä helppo muuttaa.	**OK**
Lokitus on toteutettu järjestelmässä niin, että toimista kerätään useampaa erilaista lokia (onnistuneet tai epäonnistuneet aktiviteetit, virhetilanteet jne.). Näistä lokeista on teoriassa mahdollista selvittää, mitä järjestelmässä on tehty tiettynä ajanhetkenä. Lokeja on teoriassa mahdollista väärentää, jos sovittu ylläpitomalli pettäisi. Tämä tekeminen huomaamattomasti edellyttää kuitenkin jonkin verran työtä, mikä tekee väärinkäytöstä hankalampaa.	

3 Vaalijärjestelmän kehityssuositukset

3.1 Prosessidokumentaation kehitys

Suosittelemme, että jatkossa vaalijärjestelmän prosessidokumentaation yksityiskohtaisuutta lisätään sellaiselle tasolle, että jokainen vaaleihin liittyvä käyttötapaus on dokumentoitu siten, että ATK-ajokortin suorittanut henkilö pystyy ymmärtämään käyttötapausten toimenpiteet.

Nykyinen malli edellyttää ylläpidolta vahvaa teknistä osaamista käytetyistä ratkaisuista ja teknologioista, etenkin poikkeustilanteissa. Tulevaisuudessa on mahdollista, että ylläpitoa on tekemässä taho, joka ei ole ollut toteuttamassa järjestelmää. Näissä tapauksissa olisi tärkeää, että ohjeistus tarjoaa riittävän valmiuden järjestelmän käytölle. Muuten riskinä on sellaisten virheiden syntyminen, jotka voivat vaikuttaa vaalitulokseen.

Suosittelemme, että ongelmien ratkaisemiseen laaditaan yleisimpien ongelmatilainteiden kuvaukset ja tarkat ratkaisuehdotukset niihin.

3.2 Vaalituloksen eheyden takaaminen teknisesti

Nykyisessä mallissa järjestelmä ei teknisesti tarjoa mekanismeja siihen, että vaalituloksen luotettavuutta voisi varmistaa jälkikäteen. Sisäpiiriläisten tekemät väärinkäytökset voidaan torjua ainoastaan prosessin kautta, joka takaa lähinnä sen, ettei yksittäinen ihminen voi päästä tekemään järjestelmään muutoksia.

Nykyisen järjestelmän muuttaminen toimimaan samalla periaatteella kuin useat jo käytössä olevat järjestelmät (esim. Viron äänestysjärjestelmä) ei ole teknisesti kovin helppoa. Mittavat muutokset äänien antamiseen, tallentamiseen ja laskemiseen johtaisivat käytännössä siihen, että koko järjestelmä tulisi toteuttaa uudelleen ja sen toteutus olisi merkittävästi hankalampi teknisesti.

Sähköinen äänestys alueena kehittyy jatkuvasti ja sinne syntyy uusia tuotteita sekä ratkaisuja, jotka saatavat jossain vaiheessa sellaisenaan tai pienin muutoksin tarjota korvaavan ratkaisun. On suositeltavaa seurata kehitystä ja harkita myöhemmässä vaiheessa, voisiko jokin toinen ratkaisu tarjota riittävät tekniset takeet, joilla luottamus saataisiin siirrettyä sisäisestä prosessista teknologiaan.

Nykyisen järjestelmän osalta keskustelu luotettavuudesta ja vaalituloksen uskottavuudesta kääntyy lähes suoraan keskusteluksi siitä, miten uskottava ylläpidon prosessi on.