MIETINTÖJÄ JA LAUSUNTOJA
BETÄNKANDEN OCH UTLÅTANDEN

59
2017

Nettiäänestys Suomessa

Esiselvitys

OIKEUSMINISTERIÖ JUSTITIEMINISTERIET

Mietintöjä ja lausuntoja 59/2017

Nettiäänestys Suomessa

Esiselvitys

Oikeusministeriö, Helsinki 2017

Oikeusministeriö

ISBN: 978-952-259-660-4 (nid.)
ISBN: 978-952-259-661-1 (PDF)

Helsinki 2017

Kuvailulehti

Julkaisija	Oikeusministeriö		19.12.2017
Tekijät	Nettiäänestystyöryhmä 2017		
Julkaisun nimi	Nettiäänestys Suomessa Esiselvitys		
Julkaisusarjan nimi ja numero	Oikeusministeriön julkaisu 59/2017		
Diaari/hankenumero	OM024:00/2017	Teema	Mietintöjä ja lausuntoja
ISBN painettu	978-952-259-660-4	ISSN painettu	1798-7091
ISBN PDF	978-952-259-661-1	ISSN PDF	1798-7105
URN-osoite	http://urn.fi/URN:ISBN:978-952-259-661-1		
Sivumäärä	86	Kieli	suomi
Asiasanat	nettiäänestys, vaalit, demokratia		

Tiivistelmä

Oikeusministeriö asetti työryhmän valmistelemaan esiselvityksen nettiäänestyksen toteuttamisesta toimikaudelle 21.2.2017–30.11.2017. Työryhmä tuotti esiselvityksen yleisissä vaaleissa ja neuvoa-antavissa kansanäänestyksissä käytettävästä nettiäänestysjärjestelmästä ja tätä täydentävän loppuraportin. Loppuraportissa käsitellään nettiäänestyksen edellytyksiä ja mahdollisuuksia yhteiskunnallisesta näkökulmasta.

Työryhmä toteaa, että on olemassa varteenotettavia nettiäänestysjärjestelmiä, mutta niistä mikään ei täytä vaatimuksia ja jatkokehityksestäkin huolimatta kokonaistoteutukseen jää riskejä. Päätös nettiäänestyksen käyttöönotosta tulee perustua riskien hyväksymiseen.

Varmennettavuuden ja vaalisalaisuuden samanaikainen takaaminen on ongelmallista. Lisäksi äänestämiseen valvomattomissa olosuhteissa, äänestäjän tunnistamiseen ja järjestelmän toimintavarmuuteen liittyy haasteita. Keskeistä on kansalaisen luottamus.

Työryhmä ei suosittele nettiäänestyksen käyttöönottoa, koska tällä hetkellä riskit ovat suuremmat kuin hyödyt. Teknologian ja demokratian digitalisoinnin kehitystä tulee seurata ja nykyistä vaalitietojärjestelmää kehittää edelleen. Parlamentaarinen seurantaryhmä totesi, että nettiäänestystä ei tule ottaa käyttöön yleisissä vaaleissa, koska riskit ovat suurempia kuin hyödyt. Nykytilanteessa olevia ongelmia, kuten alhainen äänestysaktiivisuus, ei ratkaista nettiäänestyksellä.

Kustantaja	Oikeusministeriö
Painopaikka ja vuosi	Lönnberg Print & Promo, 2017
Julkaisun myynti/jakaja	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi

Presentationsblad

Utgivare	Justitieministeriet		19.12.2017
Författare	Arbetsgruppen 2017		
Publikationens titel	Internetröstning i Finland Förutredning		
Publikationsseriens namn och nummer	Justitieministeriets publikation 59/2017		
Diarie-/projektnummer	OM024:00/2017	Tema	Betänkanden och utlåtanden
ISBN tryckt	978-952-259-660-4	ISSN tryckt	1798-7091
ISBN PDF	978-952-259-661-1	ISSN PDF	1798-7105
URN-adress	http://urn.fi/URN:ISBN:978-952-259-661-1		
Sidantal	86	Språk	finska
Nyckelord	internetröstning, val, demokrati		

Referat

Justitieministeriet tillsatte en arbetsgrupp för förutredning om internetröstning för mandatperioden 21.2.2017–30.11.2017. Arbetsgruppen utarbetade en förutredning och en kompletterande slutrapport om ett system för internetröstning i allmänna val och referendum. I slutrapporten behandlas förutsättningarna och möjligheterna för internetröstning ur ett samhällsperspektiv.

Arbetsgruppen konstaterar att det finns potentiella system för internetröstning, men att inget av dem uppfyller kraven och att det trots vidareutveckling finns risker med dem. Beslutet om införande av internetröstning bör basera sig på accepterade risker.

Det är problematiskt att samtidigt garantera verifierbarheten och valhemligheten. Dessutom finns det problem med röstning i oövervakade förhållanden, identifiering av röstare och systemets driftssäkerhet. Medborgarnas förtroende är centralt.

Arbetsgruppen rekommenderar inte införande av internetröstning, eftersom riskerna för närvarande är större än fördelarna. Utvecklingen av tekniken och digitaliseringen av demokratin bör följas upp och det befintliga valdatasystemet vidareutvecklas. Den parlamentariska uppföljningsgruppen konstaterade att internetröstning inte bör införas i allmänna val, eftersom riskerna är större än fördelarna. Aktuella problem, såsom en låg röstningsaktivitet, löses inte genom internetröstning.

Förläggare	Justitieministeriet
Tryckort och år	Lönnberg Print & Promo, 2017
Beställningar/ distribution	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: julkaisutilaukset.valtioneuvosto.fi

Description sheet

Published by	Ministry of Justice		19 December 2017
Authors	Online voting working group 2017		
Title of publication	Online voting in Finland A feasibility study		
Series and publication number	Publication of the Ministry of Justice 59/2017		
Register number	OM024:00/2017	Subject	Memorandums and statements
ISBN (printed)	978-952-259-660-4	ISSN (printed)	1798-7091
ISBN PDF	978-952-259-661-1	ISSN (PDF)	1798-7105
Website address (URN)	http://urn.fi/URN:ISBN:978-952-259-661-1		
Pages	86	Language	Finnish
Keywords	Online voting, elections, democracy		

Abstract

The Ministry of Justice appointed a working group to conduct a feasibility study on the introduction of online voting in Finland. The term of the working group was from 21 February to 30 November 2017. In addition to carrying out a feasibility study on online voting systems that could be used in general elections and consultative referendums, the working group also drew up a complementary final report. The final report examines the preconditions for online voting and the possibilities it could offer from a societal perspective.

The working group states that viable electronic voting systems do already exist, but that none of them meets the requirements and that risks would continue to exist even after further development. The decision on the introduction of online voting must be based on the acceptance of the related risks.

According to the working group, guaranteeing verification and election secrecy at the same time is problematic. There are also challenges related to voting in an unsupervised environment, identification of voters and reliability of the system. The trust of citizens is of key importance.

The working group does not recommend the introduction of online voting in Finland, as its risks currently outweigh its benefits. The development of technology and the digitalisation of democracy must be closely followed and the current election information system further developed. The parliamentary monitoring group stated that online voting should not be introduced in general elections as the risks are greater than the benefits. The possibility for online voting would not, in any case, resolve the current problems, such as the low voter turnout.

Publisher	Ministry of Justice
Printed by (place and time)	Lönnberg Print & Promo, 2017
Publication sales/ Distributed by	Online version: julkaisut.valtioneuvosto.fi Publication sales: julkaisutilaukset.valtioneuvosto.fi

Sisältö

1 Johdanto

1.1 Esiselvityksen tausta ja tavoitteet

Pääministeri Juha Sipilän hallitus linjasi 26.10.2016 pidetyssä strategiaistunnossaan, että Suomessa valmistellaan siirtymistä nettiäänestykseen perinteisen äänestyksen rinnalla kaikissa vaaleissa. Linjauksen perusteella päätettiin tuottaa esiselvitys nettiäänestyksen käyttöönotosta yleisissä vaaleissa. Oikeusministeriö asetti työryhmän valmistelemaan esiselvityksen nettiäänestyksen toteuttamisesta ajalle 21.2.2017–30.11.2017.

Työryhmän puheenjohtajana toimi johtaja Johanna Suurpää ja varapuheenjohtajana vaalijohtaja Arto Jääskeläinen oikeusministeriöstä. Työryhmän jäsenet olivat erityisasiantuntija Markus Rahkola valtiovarainministeriöstä, päällikkö Mikko Viitaila Viestintäviraston Kyberturvallisuuskeskuksesta, it-asiantuntija Juha Mäenalusta ja erityisasiantuntija Anniina Tjurin Oikeusrekisterikeskuksesta, riskienhallintapäällikkö Tommi Simula Valtorista, kehityspäällikkö Pauli Pekkanen Väestörekisterikeskuksesta, professori Tuomas Aura Aalto yliopistosta, dosentti Seppo Virtanen Turun yliopistosta, professori Marianne Kinnula Oulun yliopistosta, akatemiatutkija Hanna Wass Helsingin yliopistosta ja Timo Karjalainen kansalaisjärjestö Electronic Frontier Finland ry EFFI:stä. Työryhmän sihteereinä toimivat projektipäällikkö Anneli Salomaa ja neuvotteleva virkamies Heini Huotarinen oikeusministeriöstä.

Työryhmälle asetettiin parlamentaarinen seurantaryhmä, jonka puheenjohtajana toimi Antti Kurvinen Keskustan eduskuntaryhmästä. Parlamentaarisessa seurantaryhmässä jäseninä olivat Jani Mäkelä (ps), Mari-Leena Talvitie (kok), Joona Räsänen (sdp), Silvia Modig (vas), Jyrki Kasvi (vihr), Eva Biaudet (rkp), Johanna Kosunen (kd) ja Simon Elo (sin).

Työryhmän tehtävänä oli tuottaa JHS 172 -suosituksen mukainen esiselvitys yleisissä vaaleissa ja neuvoa-antavissa kansanäänestyksissä käytettävästä nettiäänestysjär-

jestelmästä. Selvityksen osa-alueita ovat mm. toimintaympäristön kartoitus, markkinakartoitus, riskien tunnistaminen, tietoturvallisuuden kartoittaminen, tavoiteratkaisun tarkentaminen sekä jatkotoimenpide-ehdotuksen esittäminen.

Esiselvityksen tehtävänä on tuottaa tietoa päätöksenteon pohjaksi sekä määrittää lähtökohdat mahdolliselle tietojärjestelmän hankinnalle. Hankkeessa tuotettiin nykytilan kuvaus, tietoturvariskien kartoitus, markkinakartoituksen osana toimittajavastausten analyysi, vaatimusmäärittely, arkkitehtuurikuvaus ja kustannusarvio.

Työryhmä kuuli prosessin aikana seuraavia henkilöitä: Tarvi Martens, Head of Internet Voting (State Electoral Office, Estonia), Tietoyhteiskunta-asiain päällikkö Tommi Karttaavi (Kuntaliitto), Kyberturvallisuuden professori Jarno Limnell (Aalto yliopisto), Kyberturvallisuuden professori Martti Lehto (Jyväskylän yliopisto) ja Hankepäällikkö Jani Ruuskanen (Väestörekisterikeskus).

Nettiäänestysjärjestelmän tietoturvallisuuden varmistaminen on ollut alusta alkaen keskeinen vaatimus. Työn aikana nousi esille vaalien toimittamiseen liittyviä, toistensa kanssa ristiriitaisia vaatimuksia, jotka edellyttävät merkittäviä toimintatapalinjauksia, ennen kuin hankintaan voi edetä. Nämä on nostettu erikseen esille päätöksentekoa varten.

2 Termit ja määritelmät

Sähköinen äänestys (electronic voting, e-voting) = äänestystapa, jossa yksi tai useampi vaihe äänestysprosessissa toteutetaan sähköisiä laitteita käyttäen. Laitteina voi olla erillinen äänestyspääte, tietokone tai mobiililaite.

Nettiäänestys (internet voting, online voting) = internet-äänestys, äänestystapa, jossa äänestys tapahtuu valvomattomissa olosuhteissa tietoverkon välityksellä.

Etä-äänestäminen (remote voting) = äänestystapa, jossa äänestäminen tapahtuu muualla kuin varsinaisella vaalipaikalla. Esimerkiksi kirjeäänestys, puhelinäänestys tai internetin välityksellä tapahtuva äänestys.

Päästä päähän varmennettavuus (end-2-end verifiability) = Periaate, jolla pyritään varmistamaan, että ääni kulkeutuu äänestystapahtumasta laskentaan asti muuttumattomana.

Yksilöllinen varmennettavuus (individual verifiability) = Äänestäjä voi varmistaa, että hänen äänensä on laskettu sen ehdokkaan hyväksi, jota hän päätelaitteellaan äänesti.

Universaali varmennettavuus (universal verifiability) = Kuka tahansa voi varmistua siitä, että kaikki äänet on laskettu oikein.

Avoin lähdekoodi (open source) = Avoin lähdekoodi on tapa kehittää ja jaella tietokoneohjelmistoja. Avoimen lähdekoodin ohjelmistoa saa vapaasti käyttää, kopioida, muunnella ja jakaa.

Proof of Concept (Poc) = tehdään minimitoiminnallisuus, jolla voidaan todentaa suoritukseen liittyvä kokonaisprosessi.

Saas (Software as Service) = ohjelmiston hankkiminen palveluna perinteisen lisenssipohjaisen hankinnan sijaan.

3 Nykytilan kuvaus

3.1 Suomen vaalijärjestelmä

Suomessa toimitetaan seuraavat yleiset valtakunnalliset vaalit:

- eduskuntavaalit joka neljäs vuosi,
- kuntavaalit joka neljäs vuosi,
- tasavallan presidentin vaali (presidentinvaali) joka kuudes vuosi ja
- Euroopan parlamentin vaalit (europarlamenttivaalit) joka viides vuosi.

Maakunta- ja soteuudistuksen (HE 15/2017 vp) myötä näiden edellä mainittujen lisäksi on tulossa maakuntavaalit, joissa äänestetään maakuntavaltuustot maakunnallisille itsehallintoalueille.

Vaalien lisäksi voidaan toimittaa myös yleiseen äänestysoikeuteen perustuvia

- neuvoa-antavia valtiollisia kansanäänestyksiä ja
- neuvoa-antavia kunnallisia kansanäänestyksiä.

Neuvoa-antavia valtiollisia kansanäänestyksiä on järjestetty Suomen historiassa vain kaksi kertaa. Ensimmäinen koski kieltolain kumoamista vuonna 1931 ja toinen Euroopan Unioniin liittymistä 1994. Valtiollinen kansanäänestys voidaan toimittaa valtiollisten vaalien yhteydessä tai vaaleista erillisenä.

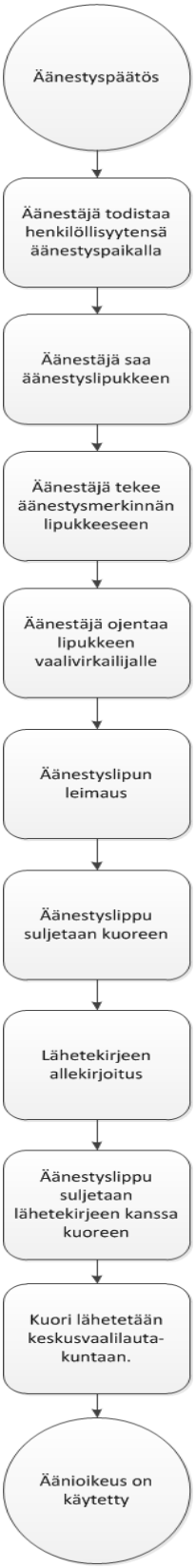
Myös kunnallinen kansanäänestys on neuvoa-antava. Sillä ei siksi ole samaa sitovaa oikeudellista luonnetta. Kansanäänestyksen toimeenpanosta päättää valtuusto. Kuntalainen voi tehdä aloitteen kunnallisen kansanäänestyksen järjestämisestä. Jos kansanäänestystä kannattaa vähintään 4 prosenttia kunnan kaikista 15 vuotta täyttäneistä asukkaista, valtuuston on käsiteltävä aloite. Kunnallisen kansanäänestyksen järjestämiselle ei ole erityisiä rajoituksia, mutta kansanäänestystä ei saa järjestää valtiollisten vaalien tai kuntavaalien yhteydessä.

Kaikki Suomen yleiset vaalit toimitetaan noudattaen seuraavia periaatteita:

- Vaalit ovat välittömät. Valitsijat (äänioikeutetut) äänestävät suoraan niitä henkilöitä, jotka he tahtovat saada valituiksi.
- Vaalit ovat suhteelliset. Suhteellisissa vaaleissa jokainen puolue (tai muu ryhmittymä) saa sen määrän edustajia kuin mitä sen vaaleissa saama äänimäärä suhteessa muihin ryhmittymiin edellyttää. Jos esimerkiksi puolue saa annetuista äänistä 20 prosenttia, sen tulisi saada myös 20 prosenttia jaettavina olevista edustajanpaikoista. (Tämä ei koske presidentinvaalia, jossa äänestetään vain asetettuja ehdokkaita, ei puolueita).
- Vaalit ovat salaiset. Vaalisalaisuudella tarkoitetaan, etteivät sen enempää vaaliviranomaiset kuin ketkään muutkaan saa tietää, ketä äänestäjä on äänestänyt, vai onko hän jättänyt tyhjän äänestyslipun.
- Vaaleissa on yleinen ja yhtäläinen äänioikeus. Yleisellä äänioikeudella tarkoitetaan sitä, että äänioikeus on riippuvainen vain sellaisista edellytyksistä, jotka kansalaisilla yleensä on. Esimerkiksi äänioikeudelle eduskuntavaaleissa on vain kaksi edellytystä: 18 vuoden ikä ja Suomen kansalaisuus. Yhtäläisellä äänioikeudella tarkoitetaan sitä, että jokaisella äänioikeutetulla on yhtäläinen oikeus vaikuttaa vaalin tulokseen eli sama äänimäärä. Yleisissä vaaleissa kullakin on yksi ääni.
- Kunkin äänestäjän on äänestettävä itse. Äänioikeutta ei saa käyttää asiamiehen välityksellä.
- Äänestämisen on tapahduttava vaaliviranomaisen edessä. Tällä pyritään turvaamaan vaalien yleistä luotettavuutta, äänestäjän vapaan tahdon ilmaisemista ja myös vaalisalaisuutta. Vaaliviranomaiset ovat pääasiassa luottamushenkilöitä.
- Suomen vaalijärjestelmä on henkilö- ja puoluevaalin yhdistelmä, jossa samalla yhdellä numerolla äänestetään sekä puoluetta että henkilöä. (Tämä ei koske presidentinvaalia, jossa äänestetään vain henkilöä, ei puoluetta).

3.2 Nykyiset äänestysprosessit

Nyt käytössä olevat äänestysmuodot ovat erilaiset ennakkoäänestykset (yleinen ennakkoäänestys, koti-, laitos-, ja laivaäänestys) sekä vaalipäivän äänestys. Kirjeäänestyksen käyttöönottoa valmistellaan parhaillaan. Se tulee olemaan yksi ennakkoäänestyksen muoto.



Äänioikeusrekisterin perustaminen ja ilmoituskortin lähetys

Väestörekisterikeskus laatii äänioikeutetuista atk-perusteisen rekisterin (äänioikeusrekisteri) 46. päivänä ennen vaalipäivää. Äänioikeusrekisteriin otetaan jokaisesta äänioikeutetusta ne tiedot (muun muassa nimi, henkilötunnus, vaalipiiri, kotikunta ja äänestyspaikka), jotka olivat väestötietojärjestelmässä 51. päivänä ennen vaalipäivää.

Jokaiselle rekisteriin otetulle postitetaan viimeistään 24. päivänä ennen vaalipäivää ilmoitus äänioikeudesta (ilmoituskortti), jossa mainitaan muun muassa vaalipäivä, ennakkoäänestyspäivät, äänioikeutetun äänestyspaikan osoite sekä vaaliviranomaisten yhteystiedot.

Jos äänioikeutetulla on ulkomainen osoite väestötiedoissa, ilmoituskortti, johon kotikunta on merkitty, lähetetään tähän osoitteeseen. Ulkomaalaisissa osoitteissa on paljon virheitä, koska äänioikeutetut eivät ilmoita osoitteenmuutoksesta heidän muuttaessa toiseen osoitteeseen ulkomailla. Ilmoituskortin ei tarvitse kuitenkaan olla mukana äänestettäessä. Äänestäjät eivät tosin aina tiedä kotikuntaansa, mikä voi johtaa äänen hylkäämiseen tai siihen, että ääni ei kohdistu sille ehdokkaalle, jota äänestäjä oli halunnut äänestää.

Ennakkoäänestys

Ennakkoäänestys alkaa keskiviikkona 11. päivänä ennen vaalipäivää ja lopetetaan tiistaina 5. päivänä ennen vaalipäivää. Kotimaan yleisiä ennakkoäänestyspaikkoja ovat kunnan määräämät paikat mm. virastot, postikonttorit ja muut paikat. Yleisessä ennakkoäänestyspaikassa voi äänestää kuka tahansa äänioikeutettu riippumatta siitä, missä kunnassa hän asuu.

Kuva 1: Äänestysprosessi

Jos äänioikeutettu on ennakkoäänestyksen aikaan hoidettavana sairaalassa tai ympärivuorokautista hoitoa antavissa sosiaalihuollon toimintayksiköissä (esimerkiksi vanhainkodissa, hoivakodissa, palvelutalossa) tai otettu rangaistuslaitokseen, hän voi äänestää ennakkoon laitosäänestyksessä. Kunnanhallituksen nimeämä vaalitoimikunta saapuu kuhunkin kunnan alueella olevaan laitokseen toimittamaan äänestyksen vähintään yhtenä ja enintään kahtena ennakkoäänestysajanjaksoon sattuvana päivänä.

Henkilö saa äänestää ennakkoon kotonaan, mikäli hänen kykynsä liikkua ja toimia on siinä määrin rajoittunut, ettei hän pääse kotimaan ennakkoäänestyspaikkaan tai vaalipäivänä äänestyspaikkaan ilman kohtuuttomia vaikeuksia. Tällöin hänen luokseen saapuu sovittuna ajankohtana kunnan keskusvaalilautakunnan nimeämä vaalitoimitsija, joka ottaa äänestyksen vastaan.

Ennakkoäänestys järjestetään myös suomalaisilla laivoilla, jotka ovat poissa Suomesta kotimaan ennakkoäänestysajanjaksona ja vaalipäivänä. Laivaäänestys voidaan aloittaa viikkoa aikaisemmin kuin muu ennakkoäänestys. Laivaäänestyksessä saa äänestää vain laivan henkilökunta.

Äänestäminen tapahtuu vaaliviranomaisen valvonnassa. Äänestäjän tulee todistaa henkilöllisyytensä äänestyspaikalla. Tehtyään äänestysmerkinnän äänestyskopissa tai muuten vaalisalaisuuden säilyttäen äänestäjä esittää taitetun äänestyslipun vaaliviranomaisen vaalileimasimella leimattavaksi ja sulkee sen jälkeen äänestyslipun vaalikuoreen. Sen jälkeen äänestäjä ja vaaliviranomainen allekirjoittavat äänestäjän henkilötiedot sisältävän lähetekirjeen ja vaaliviranomainen sulkee vaalikuoren yhdessä lähetekirjeen kanssa lähetekuoreen. Äänioikeus merkitään käytetyksi sähköiseen äänioikeusrekisteriin tai jos sitä ei ole käytössä, äänioikeuden käyttö merkitään myöhemmin vaalitietojärjestelmään keskusvaalilautakunnassa. Vaaliviranomainen lähettää postitse lähetekuoren kunnan keskusvaalilautakunnalle. Tullakseen huomioon otetuksi lähetekuoren on saavuttava kunnan keskusvaalilautakunnalle viimeistään äänestyspäivää edeltävänä perjantaina ennen kello 19.

Ennakkoäänten vastaanotto

Keskusvaalilautakunta avaa saapuneen lähetekuoren, tarkastaa lähetekirjeen tietojen perusteella äänioikeusrekisteristä, että henkilöllä on äänioikeus ja ettei hän ole jo äänestänyt. Sen jälkeen hyväksyttävä vaalikuori erotetaan lähetekirjeestä. Hyväksytyt vaalikuoret siirretään tuloslaskentaan.

Vaalipäivänä äänestäminen

Vaalipäivänä äänestettäessä äänestäminen tapahtuu asuinpaikan mukaan määräytyvässä äänestyspaikassa. Vaaliluetteloista on poistettu ennakkoon äänestäneet, jolloin äänestysoikeus jää vai niille, jotka eivät ole vielä äänestäneet ennakkoäänestyksessä. Tehtyään äänestysmerkinnän äänestyskopissa tai muuten vaalisalaisuuden säilyttäen äänestäjä esittää taitetun äänestyslipun vaalilautakunnan jäsenen leimattavaksi. Sen jälkeen äänestäjä itse pudottaa äänestyslipun vaaliuurnaan.

Ulkomailla äänestäminen

Ulkomailla äänestäminen tapahtuu ulkomailla sijaitsevissa ennakkoäänestyspaikoissa, joita ovat valtioneuvoston asetuksella säädetyt edustustot ja niiden toimipaikat. Äänestääkseen ulkomailla äänioikeutetun tulee todistaa henkilöllisyytensä. Tähän käy myös ulkomainen henkilöllisyystodistus, jos siitä käy ilmi riittävät tiedot (nimi, syntymäaika). Ulkomailla äänestettäessä henkilön äänioikeus varmistetaan ja merkitään käytetyksi vasta, kun ennakkoäänestysasiakirjat saapuvat keskusvaalilautakuntaan ja henkilö on tunnistettu ja äänioikeus varmistettu. Äänestysprosessi on samanlainen kuin kotimaan ennakkoäänestyksessä ja äänen sisältävä lähetekuori lähetetään äänioikeutetun kotikunnan tai väestökirjanpitokunnan keskusvaalilautakunnalle.

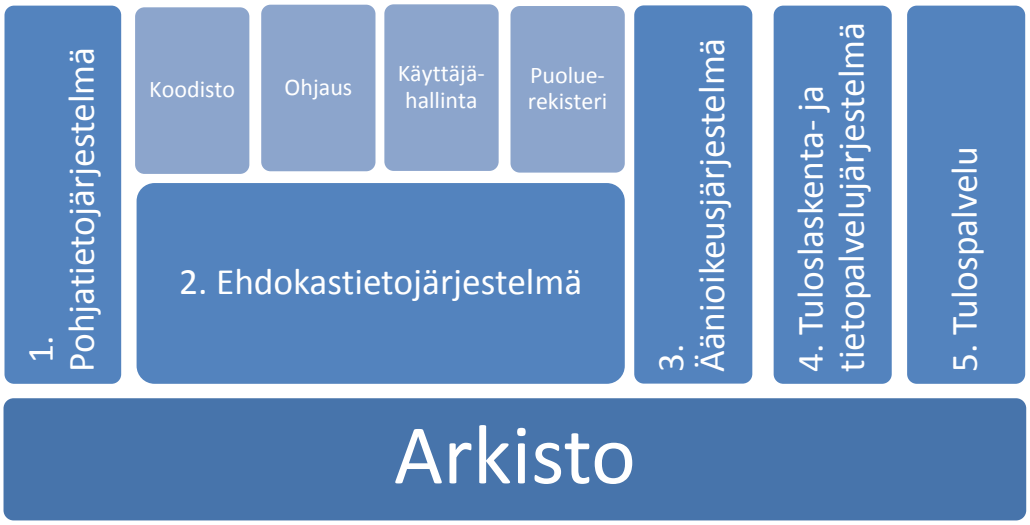
Ääntenlaskenta

Ennakkoäänten laskenta alkaa vaalipäivänä aikaisintaan kello 12 vaalipiirilautakunnassa tai kuntavaaleissa keskusvaalilautakunnassa. Kun vaalihuoneistot sulkeutuvat sunnuntai-iltana klo 20, on ennakkoäänet tähän mennessä yleensä laskettu. Äänestyspaikan sulkeuduttua vaalilautakunta suorittaa vaalipäivän äänestyslippujen alustavan laskennan ja tarkistaa, että äänestyslippujen määrä vastaa niiden henkilöiden määrää, jotka on vaaliluetteloon merkitty äänestäneiksi. Sen jälkeen tiedot äänestäneiden määrästä ja äänestyksen alustavasta tuloksesta välitetään vaalitietojärjestelmään osaksi valtakunnallista tuloslaskentaa. Maanantaina suoritetaan tarkistuslaskenta, ja lopullinen vaalitulos vahvistetaan keskiviikkona viimeistään kello 18 aloitettavassa vaalipiirilautakunnan (kuntavaaleissa keskusvaalilautakunnan) kokouksessa.

Vaaleihin liittyvät tietojärjestelmät

Vaalien toimittamiseen liittyvää tietojenkäsittelyä on kehitetty Suomessa jo pitkään. Vuonna 1972 kokeiltiin Kauniaisissa sähköistä äänestyskonetta kunnallisvaaleissa ja 70-luvun loppupuolella kehiteltiin vaalien tuloslaskentaan ja tiedottamiseen järjestelmää. Tietojärjestelmien hyödyntämisen tavoitteena on ollut vaalivalmiuden ja vaalivarmuuden parantaminen, vaaleja koskevan tietopalvelun monipuolistaminen ja no-

peuttaminen sekä resurssisäästöt. Kehittämistyön tuloksena on vuoden 1996 vaaleista lähtien ollut käytössä vaalitietojärjestelmä (VAT), joka koostuu viidestä varsinaisesta osajärjestelmästä ja arkistosta.



Kuva 2: Vaalitietojärjestelmä

1. Pohjatietojärjestelmä, jossa ovat tiedot mm. vaalipiiri-, kunta- ja äänestysaluejaoista, vaaliviranomaisista sekä tiedot yleisistä ennakkoäänestyspaikoista ja vaalipäivän äänestyspaikoista.

2. Ehdokastietojärjestelmä, jossa kuvataan jokaisesta vaaleissa ehdokkaana olevasta henkilöstä keskeiset tiedot: nimi, ehdokasnumero, ammatti, kotikunta, puolue/valitsijayhdistys, jonka ehdokkaana hän on sekä henkilötunnus. Ehdokastietojärjestelmä sisältää myös puoluerekisterin sekä kaikkia osajärjestelmiä palvelevat osat (käyttäjähallinta, koodisto, ohjaus).

3. Äänioikeustietojärjestelmä (äänioikeusrekisteri), johon poimitaan Väestörekisterikeskuksen ylläpitämästä väestötietojärjestelmästä (VTJ) vaaleissa äänioikeutettujen henkilöiden tiedot. Äänioikeusrekisteri ei ole staattinen rekisterikokonaisuus, vaan se perustetaan kutakin vaalia varten erikseen. Jokaiselle rekisteriin otetulle henkilölle lähetetään postitse vaalikohtainen ilmoituskortti. Äänioikeusrekisteri tulee lainvoimaiseksi 12. päivänä ennen vaalipäivää. Äänioikeusrekisteri on käytössä ennakkoäänestyspaikoissa ja jokaisen ennakkoon äänestävän äänestämisestä tehdään siihen merkintä. Ennakkoäänestyksen jälkeen rekisteristä tulostetaan vaaliluettelot vaalipäivän äänestyspaikoille. Sähköistä äänioikeusrekisteriä voidaan myös käyttää äänestyspai-

kalla vaaliluetteloiden sijasta tai niiden rinnalla. Vaalien jälkeen äänioikeusrekisterin tiedot hävitetään.

4. Tuloslaskentajärjestelmä, johon vaalipiirilautakunnat ja kuntien keskusvaalilautakunnat syöttävät vaalien tulostiedot sitä mukaan kuin ne valmistuvat.

5. Tulospalvelujärjestelmä, jonka avulla vaalien tulostiedot ja muut vaalitiedot välitetään tiedotusvälineille ja Tilastokeskukselle.

Arkisto, johon talletetaan jokaisen toteutetun vaalin arkistokopio.

Nykyinen vaalitietojärjestelmä alkaa olla päivityksen tarpeessa ja sen jonkin asteinen uudistaminen on lähivuosina tulossa ajankohtaiseksi. Vuoden 2018 aikana käynnistyy esiselvitys, jossa määritellään uudistuksen laajuus. Sähköisen vaaliluettelon, rajapintojen ja käyttöliittymän saavutettavuuden kehittäminen ovat muutamia tunnistettuja kehitysaskeleita. Sähköisen vaaliluettelon laajempi käyttöönotto edellyttää äänestyspaikkojen tietoteknisten valmiuksien parantamista. Nettiäänestyssovellus toteutettaisiin kuitenkin vaalitietojärjestelmästä erillisenä kokonaisuutena ja sen arkkitehtuurissa on tarkoitus minimoida riippuvuudet ulkopuolisiin järjestelmiin, joten nettiäänestysprojektissa ei kehitysvaiheiden yhteensovittamisen lisäksi olisi varsinaisia riippuvuuksia vaalitietojärjestelmän uudistamisprojektiin.

4 Lait, standardit ja suositukset

4.1 Perusoikeudet ja vaalilainsäädäntö

Nettiäänestys edellyttää vaalilainsäädännön laajamittaista muuttamista ja läpikäymistä. Lainsäädännön muutostarpeita tulee selvittää muun muassa nettiäänestysjärjestelmän ominaisuuksien, äänestäjän tunnistamisen, vaaliviranomaisten tehtävien ja vaalien muutoksenhaun näkökulmasta. Lainsäädännön kehittäminen on syytä tehdä rinnan nettiäänestysjärjestelmän kehittämisen kanssa. Perustuslaki määrittelee rajat sille, miten lainsäädäntöä voidaan muuttaa.

Perustuslain 2 §:n 1 momentissa säädetään, että valtiovalta Suomessa kuuluu kansalle, jota edustaa valtiopäiville kokoontunut eduskunta.

Perustuslain 6 §:ssä säädetty yhdenvertaisuus vaikuttaa nettiäänestyksen kehittämiseen. Ketään ei saa ilman hyväksyttävää perustetta asettaa eri asemaan sukupuolen, iän, alkuperän, kielen, uskonnon, vakaumuksen, mielipiteen, terveydentilan, vammaisuuden tai muun henkilöön liittyvän syyn perusteella. Erilaisten ryhmien tarpeet on otettava huomioon nettiäänestysjärjestelmässä. Nettiäänestäminen ei saa asettaa äänestäjiä eri asemaan esimerkiksi asuinpaikasta, iästä tai terveydentilasta riippuen. Mikäli kehittämisvaiheessa nettiäänestystä olisi tarkoituksenmukaista kokeilla esimerkiksi rajatulla maantieteellisellä alueella, asiaa tulisi arvioida myös perustuslain yhdenvertaisuussääntelyn näkökulmasta. Nettiäänestyksen hyötynä saattaisi kuitenkin olla äänestäjien tosiasiallisen yhdenvertaisuuden paraneminen äänestysmahdollisuuksien suhteen.

Vaalien ja siten myös nettiäänestyksen kannalta keskeinen perustuslain kohta on vaali- ja osallistumisoikeuksia koskeva 14 §. Siinä säädetään, että jokaisella Suomen kansalaisella, joka on täyttänyt kahdeksantoista vuotta, on oikeus äänestää valtiollisissa vaaleissa ja kansanäänestyksessä. Suomen kansalaisten lisäksi maassa asuvalla muulla Euroopan unionin kansalaisella, joka on täyttänyt kahdeksantoista vuotta, on oikeus äänestää Euroopan parlamentin vaaleissa sen mukaan kuin lailla sääde-

tään. Kansalaisilla sekä maassa vakinaisesti asuvalla ulkomaalaisella, joka on täyttänyt kahdeksantoista vuotta, on oikeus äänestää kunnallisvaaleissa ja kunnallisessa kansanäänestyksessä sen mukaan kuin lailla säädetään. Julkisen vallan tehtävänä on edistää yksilön mahdollisuuksia osallistua yhteiskunnalliseen toimintaan ja vaikuttaa häntä itseään koskevaan päätöksentekoon.

Perustuslain 24 §:n 2 momentin mukaan eduskunnan toimikausi alkaa, kun eduskuntavaalien tulos on vahvistettu, ja jatkuu, kunnes seuraavat eduskuntavaalit on toimitettu. Vaikka vaaleissa havaittaisiin väärinkäytöksiä, uusi eduskunta olisi päätösvaltainen siihen saakka, kunnes tuomioistuin määräisi uudet vaalit ja ne toimitettaisiin. Tämä seikka tulee ottaa huomioon nettiäänestyksen riskien arvioinnissa.

Perustuslain 26 §:n mukainen mahdollisuus ennenaikaisiin eduskuntavaaleihin tulee ottaa myös huomioon. Vastaava mahdollisuus liittyy tasavallan presidentin ennenaikaiseen vaaliin. Perustuslain 55 §:n 3 momentin mukaan, jos presidentti kuolee tai valtioneuvosto toteaa hänet pysyvästi estyneeksi hoitamaan presidentintointa, on niin pian kuin mahdollista valittava uusi presidentti. Nettiäänestysjärjestelmä tulee siis voida ottaa käyttöön melko lyhyellä varoitusajalla, mikäli ennenaikaiset eduskuntavaalit määrätään (lyhimmillään 51 päivää) tai tasavallan presidentti estyy pysyvästi hoitamasta tointaan.

Valtiollisten kansanäänestysten järjestämisestä säädetään perustuslain 53 §:n 1 ja 2 momentissa. Neuvoa-antavan kansanäänestyksen järjestämisestä päätetään erikseen lailla, jossa on säädettävä äänestyksen ajankohdasta ja äänestäjille esitettävistä vaihtoehdoista.

Tasavallan presidentin valinnasta säädetään perustuslain 54 §:ssä. Presidentti valitaan välittömällä vaalilla syntyperäisistä Suomen kansalaisista kuuden vuoden toimikaudeksi. Presidentiksi valitaan ehdokas, joka saa vaalissa enemmän kuin puolet annetuista äänistä. Jos kukaan ehdokkaista ei ole saanut enemmistöä annetuista äänistä, toimitetaan uusi vaali kahden eniten ääniä saaneen ehdokkaan välillä. Presidentiksi valitaan tällöin uudessa vaalissa enemmän ääniä saanut ehdokas. Vaalin ajankohdasta ja presidentin valitsemisessa noudatettavasta menettelystä säädetään tarkemmin lailla.

Järjestelmän omistajuutta ja hallinnointia arvioitaessa tulee selvitettäväksi, mitä tehtäviä ostetaan yksityisiltä tietojärjestelmätoimittajilta. Perustuslain 124 §:n mukaan julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle. On

pohdittava, kuinka paljon nettiäänestysjärjestelmän hallinnointivastuuta voidaan antaa ulkopuoliselle toimijalle.

Valtiosääntöoikeuden professori Tuomas Ojasen arvio vuosien 2014–2015 Nettiäänestystyöryhmän loppuraportin (28/2015) mukaan on, että perustuslain näkökulmasta nettiäänestykselle ei lähtökohtaisesti ole estettä, kunhan tietyt reunaehdot otetaan huomioon ja vaalien perusperiaatteet, yhdenvertaisuus, luotettavuus ja vaalisalaisuuden säilyttäminen, toteutuvat. Ojasen mukaan nettiäänestystä voidaan arvioida mm. perustuslain 6 § (yhdenvertaisuus), 9 § (liikkumisvapaus), 10 § (henkilötietojen suoja, luottamuksellisen viestinnän suoja), 14 § (vaali- ja osallistumisoikeudet), 21 § (oikeusturva), 22 § (perusoikeuksien turvaaminen), 27 § (vaalikelpoisuus), 53 § (kansanäänestys ja kansalaisaloite), 121 § (kunnallinen ja muu alueellinen itsehallinto) ja 124 § (hallintotehtävän antaminen muulle kuin viranomaiselle) näkökulmasta.

4.2 Äänioikeus

Eduskuntavaaleissa ja **presidentinvaalissa** äänioikeutettu on asuinpaikastaan riippumatta jokainen Suomen kansalainen, joka viimeistään vaalipäivänä täyttää 18 vuotta.

Kuntavaaleissa äänioikeutettu on jokainen viimeistään vaalipäivänä 18 vuotta täyttävä henkilö, joka on

a) Suomen tai muun EU:n jäsenvaltion taikka Islannin ja Norjan kansalainen ja jonka kotikunta kyseinen kunta on 51. päivänä ennen vaalipäivää; tai

b) muun valtion kansalainen, jonka kotikunta kyseinen kunta on 51. päivänä ennen vaalipäivää ja jolla on ollut yhtäjaksoisesti kotikunta Suomessa kahden vuoden ajan laskettuna 51. päivästä ennen vaalipäivää; tai

c) EU:n tai Suomessa toimivan kansainvälisen järjestön palveluksessa ja jolla on asuinpaikka kyseisessä kunnassa 51. päivänä ennen vaalipäivää edellyttäen, että hänen tietonsa on tallennettu hänen pyynnöstään väestötietojärjestelmään ja että hän on kirjallisesti ilmoittanut maistraatille viimeistään 52. päivänä ennen vaalipäivää haluavansa käyttää äänioikeuttaan kuntavaaleissa.

Äänioikeus kuntavaaleissa on sidottu asianomaisessa kunnassa asumiseen. Siten esimerkiksi pysyvästi ulkomailla asuvat suomalaiset (ulkosuomalaiset) eivät ole äänioikeutettuja kuntavaaleissa, vaikka ovatkin Suomen kansalaisia.

Suomessa toimitettavissa **europarlamenttivaaleissa** äänioikeutettu on jokainen viimeistään vaalipäivänä 18 vuotta täyttänyt

a) Suomen kansalainen asuinpaikkaan katsomatta, ja

b) muun EU:n jäsenvaltion kansalainen, joka ei ole menettänyt vaalikelpoisuuttaan kotivaltiossaan, joka on viimeistään 80. päivänä ennen vaalipäivää ilmoittautunut maistraatille otettavaksi Suomen äänioikeusrekisteriin ja

b1) jolla on kotikunta Suomessa 51. päivänä ennen vaalipäivää tai

b2) joka on EU:n tai Suomessa toimivan kansainvälisen järjestön palveluksessa tai tällaisen henkilön perheenjäsen, joka asuu Suomessa.

Suomen kansalainen, joka on säädetyssä määräajassa ilmoittautunut äänestäjäksi jonkun toisen EU:n jäsenvaltion europarlamenttivaaleissa, ei ole äänioikeutettu Suomen europarlamenttivaaleissa. Äänioikeutettu saa samoissa europarlamenttivaaleissa äänestää vain yhdessä EU:n jäsenvaltiossa: joko kotivaltiossaan tai siinä valtiossa, jossa asuu (asuinvaltiossaan). EU:n jäsenvaltioiden vaaliviranomaiset vaihtavat keskenään tietoja niistä EU-kansalaisista, jotka ovat ilmoittautuneet äänestäjiksi asuinvaltionsa europarlamenttivaaleihin.

Kukin äänioikeutettu voi oman valintansa mukaan äänestää ennakkoon missä tahansa yleisessä ennakkoäänestyspaikassa kotimaassa tai ulkomailla. (vaalilaki 4 ja 9 §).

Vaalipäivänä kukin äänioikeutettu saa äänestää vain omassa äänestyspaikassaan (vaalilaki 71 §). Vaalipäivän äänestyspaikka mainitaan äänioikeutetun postitse saamassa ilmoituskortissa (vaalilaki 21 §). Vaalipäivän äänestyksen järjestelyistä äänestyspaikalla vastaa kunnanhallituksen nimittämä vaalilautakunta. Vaalipäivän äänestyksessä äänioikeus tarkistetaan vaaliluettelosta, jossa näkyvät äänestysalueen äänioikeutetut ja ennakkoon äänestäneet.

Jokaisen on äänestettävä henkilökohtaisesti. Äänioikeutta ei saa käyttää asiamiehen välityksellä (vaalilaki 2 §). Äänestäjä saa kuitenkin käyttää apunaan valitsemaansa avustajaa äänestysmerkinnän tekemisessä. Avustaja on velvollinen tunnollisesti täyttämään äänestäjän osoitukset sekä pitämään salassa äänestyksen yhteydessä saamansa tiedot (vaalilaki 58 § ja 73 §).

Ääntenlaskenta

Valtiollisissa vaaleissa edellisissä vaaleissa ehdokkaita asettaneiden puolueiden edustajista muodostetut viisijäseniset vaalipiirilautakunnat (vaalilaki 11 §) huolehtivat ennakkoäänestyksessä annettujen äänestyslippujen laskennasta ja vaalipäivänä annettujen äänestyslippujen tarkastuslaskennasta. Kuntavaaleissa näistä tehtävistä huolehtivat edellisissä kuntavaaleissa ehdokkaita asettaneiden äänestäjäryhmien edustajista muodostetut viisijäseniset kuntien keskusvaalilautakunnat (vaalilaki 13 §), joita on jokaisessa kunnassa yksi.

Vaalien tulos lasketaan äänestysalueittain (vaalilaki 86.2 §). Kunta päättää äänestysalueiden lukumäärästä ja sijainnista (vaalilaki 8 ja 9 §). Äänestysalueet voivat olla keskenään hyvin erikokoisia. Pienimmillä äänestysalueilla on vain joitakin kymmeniä äänioikeutettuja, kun taas suurimmilla äänestysalueilla äänioikeutettuja on useita tuhansia. Hyvin pienillä äänestysalueilla vaalisalaisuuden toteutuminen voi olla epävarmaa. Vaalisalaisuuden turvaamiseksi vaalilain 82 §:ssä on säädetty, että pienten äänestysalueiden ennakkoon annetut ja vaalipäivän äänet voidaan laskea yhdessä tai äänestysalueen äänet voidaan laskea yhdessä toisen äänestysalueen äänten kanssa.

Vaalilaissa todetaan, että mikäli ennakkoääniä on hyväksytty alle 50, äänet yhdistetään vaalipäivän äänten kanssa. Netin kautta annettuja ääniä ei voi suoraan yhdistää paperiäänten kanssa, joten ne muodostavat oman tuloksensa. Mikäli tämä tulos on yhteensä alle 50, tulisi olla mahdollista yhdistää äänet yhteen tai useampaan alueeseen nettiäänestysjärjestelmässä. Tämä tarkoittaa, että vastaavat alueet yhdistetään myös paperilaskennassa.

Äänestysliput ovat anonyymeja, joten äänestäjä ei voi jälkikäteen varmistua, että hänen antamansa ääni on mukana tuloksissa. Äänestyslippujen anonymiteetti varmistetaan sillä, että äänestysliput, joissa on asiattomia merkintöjä, hylätään (vaalilaki 85 §). Toisaalta vaalituloksen julkaiseminen äänestysalueittain mahdollistaa äänestäjälle joissakin tapauksissa äänen perillemenon varmistamisen: Mikäli ehdokas, jota äänestäjä on äänestänyt, ei olisi laskennassa saanut yhtään ääntä, äänestäjä näkee tulostiedoista, ettei hänen antamansa ääni ole tullut mukaan laskentaan.

Muutoksenhausta vaaleissa säädetään vaalilain 8 luvussa. Vaalien tuloksesta voi valittaa vaaleista kuntavaaleissa, eduskuntavaaleissa ja europarlamenttivaaleissa. Presidentinvaaleissa tulokseen ei voi valittamalla hakea muutosta. Valituksen voi tehdä sillä perusteella, että vaalipiirilautakunnan tai kuntavaaleissa kunnan keskusvaalilautakunnan päätös on lainvastainen ja että vaalit on toimitettu virheellisessä järjestyksessä. Jos vaaliviranomaisen päätös tai toimenpide on ollut lainvastainen ja lainvastaisuus on ilmeisesti saattanut vaikuttaa vaalien tulokseen, vaalien tulos on oikaistava tai, jos se ei ole mahdollista, vaalit on määrättävä uusittaviksi asianomai-

sessa vaalipiirissä (kuntavaaleissa kunnassa) tai europarlamenttivaaleissa koko maassa. Näin ollen, mikäli nettiäänestysjärjestelmän käytössä todetaan olleen ongelmia, nämä virheet voivat johtaa vaalien uusimiseen.

Mikäli epäiltäisiin, että tuloksia on manipuloitu, manuaalinen paperiäänten laskennan tarkistus on nopeampi toteuttaa kuin tietojärjestelmän lokien perinpohjainen tutkiminen. Käytännössä tämä tarkoittaa sitä, että vahvistettu vaalitulos on voimassa, kunnes toisin todetaan. Vaatimuksissa onkin otettava huomioon, että kaikenlainen äänten ja tulosten manipulointi tulee pystyä tunnistamaan välittömästi.

4.3 Euroopan neuvoston suositukset

Euroopan neuvoston ministerikomitea on luonut suositukset[1] jäsenvaltioille koskien sähköistä äänestystä. Suositukset hyväksyttiin alkukesästä 2017, jolloin ne korvasivat aiemmin voimassa olleet (2004) suositukset. Nämä suositukset toimivat pohjana nettiäänestysjärjestelmän teknisille vaatimuksille ja nettiäänestyksestä vastaavan organisaation järjestäytymiselle. Myös tässä esiselvityksessä on käytetty suosituksia hyväksi muun muassa vaatimusmäärittelyssä.

Suositukset jakautuvat seuraaviin aihekokonaisuuksiin: yleinen, yhtäläinen ja vapaa äänioikeus, vaalisalaisuus, sääntely ja organisaatio, läpinäkyvyys ja tarkkailu, tilivelvollisuus/varmennettavuus sekä järjestelmän luotettavuus ja turvallisuus. Vaatimuksissa on suositeltu muun muassa päästä päähän varmennettavuuden periaatteiden noudattamista:

- *Äänestäjän on voitava tarkistaa, että annettu ääni ilmaisee hänen aikomuksensa paikkansapitävästi ja että sinetöity ääni on viety sähköiseen vaaliuurnaan sellaisenaan. Mahdolliset ääntä asiattomasti muuttaneet seikat on voitava havaita.*
- *Järjestelmän tulee antaa äänestäjälle vahvistus siitä, että äänen antaminen onnistui ja että äänestysmenettely on saatettu päätökseen.*
- *Sähköisen äänestysjärjestelmän on annettava pitävä todiste siitä, että jokainen aito ääni on paikkansapitävästi sisällytetty vaalitulokseen. Todisteet on voitava tarkistaa käyttäen keinoja, jotka ovat riippumattomia sähköisestä äänestysjärjestelmästä.*

[1] Recommendation CM/Rec(2017)5[1] of the Committee of Ministers to member States on standards for e-voting
(Adopted by the Committee of Ministers on 14 June 2017 at the 1289th meeting of the Ministers' Deputies)

- *Järjestelmän on annettava pitävä todiste siitä, että ainoastaan äänioikeutettujen äänestäjien äänet on sisällytetty lopputulokseen. Todisteet on voitava tarkistaa käyttäen keinoja, jotka ovat riippumattomia sähköisestä äänestysjärjestelmästä.*

Vaalisalaisuuteen ja painostamisen estämiseen liittyen kuitenkin suositus on, ettei äänestäjä pysty todistamaan ulkopuoliselle mitä on äänestänyt.

- *Sähköisen äänestysjärjestelmän ei tule antaa äänestäjälle todistetta annetun äänen sisällöstä kolmansien osapuolten käyttöön*

Ratkaistavana on siis, kuinka tämä todiste toimitetaan ilman, että ulkopuolinen voi saada sen haltuunsa.

Suosituksissa todetaan, että ennen sähköisten vaalien käyttöönottoa on tehtävä tarvittavat muutokset merkitykselliseen lainsäädäntöön. Laissa on säänneltävä sähköisten äänestysjärjestelmien toimintaa koskevia velvollisuuksia ja vaalivalvontaelimen tehtäviä. Vaalivalvontaelimen vastuulla tulee olla muun muassa sähköisen ääntenlaskentaprosessin ja vaatimusten noudattamisen valvonta, täytäntöönpano myös häiriöiden ja hyökkäysten tapahtuessa sekä yleisesti sähköisen äänestysjärjestelmän saatavuuden, luotettavuuden, käytettävyyden ja turvallisuuden varmistaminen.

4.4 Saavutettavuus

Saavutettavuus on kohteen tai verkkopalvelun helppoa käytettävyyttä kaikille. Toteutuminen jakautuu tekniseen saavutettavuuteen ja sisällölliseen saavutettavuuteen. Tekninen saavutettavuus tarkoittaa sitä, että sisältö on teknisesti oikein toteutettu ja apuvälinein käytettävissä. Tähän on saatavilla tarkistuslistoja ja -ohjelmia. Sisällön saavutettavuudella pyritään siihen, että sisältö on ymmärrettävissä, helposti omaksuttavissa ja käytettävissä. On pidettävä mielessä, että verkkopalvelu voi olla teknisesti saavutettava, mutta siltikään käyttäjä ei pysty hyödyntämään sisältöä, jos sisällön suunnitteluun ei ole kiinnitetty huomiota.

Nettiäänestämisestä arvioidaan olevan erityistä hyötyä mm. näkövammaisille ja liikuntaesteisille. Äänestämisessä tulee varsinaisen äänestystapahtuman lisäksi ottaa huomioon koko prosessi, alkaen tunnistautumisesta ja päättyen siihen, että äänestäjä on saanut varmistuksen äänen perillemenosta. Kaikenlaiset käyttäjät tuleekin ottaa mukaan kehitystyöhön suunnittelusta alkaen ja testausta tulee koko prosessin ajan tehdä laajalle käyttäjäkunnalle. Ketterät kehitysmallit sopivat tähän erityisen hyvin. Kaikille avoimia kokeiluja ja testauksia voidaan järjestää ennen varsinaista käyttöönot-

toa vaaleissa. Kehitystyön budjetoinnissa ja aikataulutuksessa on varmistettava, että julkisessa testauksessa esille tulleet haasteet pystytään korjaamaan.

Tunnistuksen käytettävyys on varmistettava, koska verkkopalvelu ei ole saavutettava, jos käyttäjä ei onnistu kirjautumaan sisään. Eri palveluntarjoajien tunnistusvälineissä on tällä hetkellä eroja ja tavoitetila on, että käyttäjä voisi rajoitteistaan tai palveluntarjoajastaan riippumatta tunnistautua turvallisesti sähköisiin palveluihin. Tulevan EU:n esteettömyysdirektiivin[2] myötä myös sähköisten tunnistusvälineiden tulee olla esteettömästi kaikkien käytettävissä. Direktiivin voimaantulosta ei ole vielä tarkempaa aikataulua, mutta neuvoston työryhmässä on käyty neuvotteluja direktiivistä syksyn aikana ja tarkoituksena olisi aloittaa toimielinten väliset neuvottelut mahdollisesti jo tämän vuoden puolella.

Julkisia verkkopalveluja koskeva Euroopan Unionin saavutettavuusdirektiivi[3] hyväksyttiin syksyllä 2016. Saavutettavuusdirektiivin mukaan saavuttavan verkkopalvelun tulee täyttää yhdenmukaistettujen standardien vaatimukset. Direktiivin kansalliset toimeenpanopäätökset tulee olla tehtynä 23.9.2018. Verkkopalveluiden, jotka julkaistaan 23.9.2018 jälkeen, tulee olla direktiivin mukaisia 23.9.2019 ja mobiilisovellusten 23.6.2021 alkaen. Lainsäädäntö ja yhdenmukaisten vaatimusten määrittely ovat vielä kesken tätä esiselvitystä kirjoittaessa, mutta tavoiteltava taso tulee todennäköisesti olemaan tekeillä oleva eurooppalainen saavutettavuusstandardi EN 301 549[4] ja siihen yhdistettynä WGAC 2.1 määritellyt mobiilisovelluksia koskevat vaatimukset[5].

4.5 Kielilainsäädäntö

Kielilaki (423/2003) on yleislaki ja koskee koko julkista sektoria. Kaikki keskushallintoviranomaiset ovat kaksikielisiä ja niiden tulee palvella suomeksi ja ruotsiksi. Kaikessa tiedottamisessa tulee käyttää sekä suomen että ruotsin kieltä. Laki takaa oikeuden asioida viranomaisten kanssa suomeksi ja ruotsiksi, joten julkisen verkkopalvelun on oltava käytettävissä näillä molemmilla kansalliskielillä.

Enontekiön, Inarin, Sodankylän ja Utsjoen alueella saamen kielilaki (1086/2003) takaa saamelaisille oikeuden käyttää saamea tai suomea asioidessaan viranomaisen kanssa. Oikeudesta käyttää ruotsin kieltä säädetään kielilaissa (423/2003). Oikeusministe-

[2] COM (2015) 615 final, Ehdotus - Euroopan parlamentin ja neuvoston direktiivi tuotteiden ja palvelujen esteettömyysvaatimuksia koskevien jäsenvaltioiden lakien, asetusten ja hallinnollisten määräysten lähentämisestä.
[3] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/2102, annettu 26 päivänä lokakuuta 2016, julkisen sektorin elinten verkkosivustojen ja mobiilisovellusten saavutettavuudesta
[4] http://www.etsi.org/deliver/etsi_en/301500_301599/301549/01.01.02_60/en_301549v010102p.pdf
[5] https://www.w3.org/TR/WCAG21/ (Draft 16.8.2017)

riö ei kuulu viranomaisiin, joilla lain mukaan on saamen kielellä tiedottamisvelvoite. Tästä huolimatta oikeusministeriö on laatinut eräitä vaaleissa käytettäviä lomakkeita myös saamen kielellä.

Viittomakielilaissa (359/2015) määritetään, että viranomaisen on toiminnassaan edistettävä viittomakieltä käyttävän mahdollisuuksia käyttää omaa kieltään ja saada tietoa omalla kielellään.

Kielellisten oikeuksien ja osallisuuden edistäminen on perustuslain (731/1999) mukaista perusoikeuksien ja ihmisoikeuksien toteutumisen turvaamista. Tästä syystä verkkopalvelun tulee olla suomen ja ruotsin lisäksi käännettävissä myös saamen kielille ja viittomakielille. Teknisesti tämä tarkoittaa videoupotusmahdollisuutta ja saamenkielisiä fontteja.

4.6 Sähköinen tunnistautuminen

Äänestäjän on selvitettävä henkilöllisyytensä äänestyspaikalla (vaalilaki 57.2 § ja 75.2 §). Siksi hänen tulee ottaa mukaansa kuvallinen henkilöllisyystodistus, esimerkiksi sirullinen henkilökortti, ajokortti tai passi. Nettiäänestysjärjestelmässä vaaditaan vastaavasti vahvaa sähköistä tunnistusta.

Vahva sähköinen tunnistaminen, sähköinen allekirjoitus ja varmenne auttavat henkilöllisyyden todentamisessa ja tunnistamisessa sekä tietojen salauksessa sähköisissä tietoverkoissa. Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista säädetään laissa[6] .

Vahvalla sähköisellä tunnistamisella tarkoitetaan henkilöllisyyden todentamista sähköisesti. Vahvan sähköisen tunnistamisen avulla kuluttajat voivat turvallisesti vahvistaa henkilöllisyytensä erilaisissa sähköisissä palveluissa.

Varmenteita tarvitaan tietoverkkojen kautta tapahtuvassa tunnistamisessa, salauksessa ja sähköisen allekirjoituksen tekemisessä. Varmenne on luotettavan organisaation sähköisesti allekirjoittama todistus, joka todentaa varmenteen omistajan henkilöllisyyden tai palvelimen. Varmenne sisältää julkisen avaimen, jolla varmenteen omistajan voi tunnistaa. Varmenteen tietosisällöstä ja varmentajan toiminnasta on säädetty vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa.

[6] Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (2009/617)

Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain tavoitteena on luoda yhteiset pelisäännöt vahvan sähköisen tunnistamisen palvelujen tarjontaan ja edistää tunnistuspalveluiden tarjontaa ja sähköisten luottamuspalveluiden käyttöä. Lain lähtökohtana on, että käyttäjä voi luottaa vahvan sähköisen tunnistamisen tietoturvaan ja yksityisyyden suojaan.

eIDAS tuo muutoksia sähköiseen tunnistamiseen ja luottamuspalveluihin EU:ssa

EU:n eIDAS-asetuksen[7] keskeisiä tavoitteita ovat tarjota sähköisiä tunnistusvälineitä, joilla on mahdollista tunnistautua julkishallinnon palveluissa koko EU:ssa viimeistään 2018 syksyllä sekä antaa palveluntarjoajalle mahdollisuus osoittaa selkeästi, että sen verkkopalveluita varten tarjoama tuote (mm. allekirjoitusvarmenne, sähköinen aikaleima = luottamuspalvelut) on luotettava. eIDAS tuli voimaan 1.7.2016. Samanaikaisesti tulivat voimaan muutokset lakiin vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (2009/617).

Suomessa tunnistamisesta on säädetty jo aiemmin, mutta nyt sitä sovitetaan yhteen uuden EU-sääntelyn kanssa. Suomessa kansallisen tunnistamisen sääntely tulee pohjautumaan eIDAS-asetuksen rajat ylittävän tunnistamisen vaatimuksiin. Jäsenvaltioiden viranomaisten on tunnustettava toisen jäsenvaltion komissiolle ilmoittamat sähköisen tunnistamisen menetelmät. Yksinkertaistettuna tämä tarkoittaisi esimerkiksi sitä, että komissiolle ilmoitetut ruotsalaiset vahvat sähköiset tunnisteet kelpaavat suomalaisiin julkishallinnon palveluihin ja vastaavasti suomalaiset tunnistamisen välineet hyväksytään vastaaviin ruotsalaisiin palveluihin.

Pohjoismaiden ja Baltian alueen ministerit antoivat 25.4.2017 julkilausuman, jonka tavoitteena on mm. rajat ylittävä digitaalinen palvelualue julkisella sektorilla. Yhtenä toimenpiteenä mainittiin: ”Mahdollistetaan yksilöllisten henkilötunnusten käyttö yli rajojen ja helpotetaan kansallisten infrastruktuurien välistä yhteistyötä sähköisen tunnistamisen (eID) käyttämiseksi eIDAS-asetuksen mukaisesti.” Kansallisten henkilötunnuksen hyödyntämiseen yli rajojen liittyy vielä avoimia kysymyksiä ja selvityshankkeita on suunniteltu vuosille 2018–2019.

Yleisesti haasteina ovat maiden erilaiset käytännöt henkilöiden identifiointiin ja se, ettei ulkomaisesta henkilöllisyystodistuksesta saa suomalaisissa sähköisissä palveluissa tarvittavia tietoja, kuten suomalaista henkilötunnusta.

[7] Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014 , sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta

Taulukko 1: Sähköisen tunnistamisen varmuustasot (eIDAS)

Varmuustaso		Asiointipalvelun riskitaso
Matala (low)	tarjoaa rajoitetun luottamustason henkilön väitetyn tai esitetyn henkilöllisyyden osalta, ja vähentää henkilöllisyyden väärinkäytön ja muuttamisen riskiä	Virheelliseen tunnistukseen liittyy kohtalainen riski
Korotettu (substantial)	tarjoaa merkittävän luottamustason henkilön väitetyn tai esitetyn henkilöllisyyden osalta, ja vähentää merkittävissä määrin henkilöllisyyden väärinkäytön ja muuttamisen riskiä	Virheelliseen tunnistukseen liittyy merkittävä riski
Korkea (high)	tarjoaa korkeamman luottamustason henkilön väitetyn tai esitetyn henkilöllisyyden osalta kuin korotetun varmuustason omaava sähköisen tunnistamisen menetelmä, ja jonka tarkoituksena on estää henkilöllisyyden väärinkäyttö ja muuttaminen	Virheelliseen tunnistukseen liittyy korkea riski

Äänestämisen siirtyessä verkkoon ja valvomattomiin olosuhteisiin, henkilön luotettava tunnistaminen nousee keskeiseksi toiminnallisuudeksi. Henkilöllisyyden väärinkäyttö tai muuttaminen tulisi estää kaikin mahdollisin keinoin. Kuitenkaan tämäkään ei lopulta takaa sitä, että oikea henkilö käyttää tunnistusvälinettä. Biometriset tunnisteet voisivat tuoda tähän ratkaisuja, mutta teknologian käyttö ei ole vielä yleistynyt ja siinä on omat haasteensa.

Tällä hetkellä vahvoja sähköisiä tunnistusvälineitä ovat verkkopankkitunnukset (TUPAS), teleyritysten mobiilivarmenteet ja Väestörekisterikeskuksen kansalais-, organisaatio-, sosiaali- ja terveydenhuollon varmenteet. Korotetulla tasolla oleva verkkopankkitunnistus on yleisesti käytössä sähköisessä asioinnissa ja sen katsotaan riittävän tietoturvakriittiseenkin sähköiseen asiointiin. Tietoturvariskit on nettiäänestysjärjestelmälle tehdyn alustavan luokittelun perusteella arvioitu kuitenkin niin suuriksi, että korkea taso on tietoturvanäkökulmasta perusteltu.

Korkean tason varmennekortti ei ole kopioitavissa ja sen lisäksi kortissa on allekirjoitusvarmenne ja yksityinen allekirjoitusavain, joilla voidaan allekirjoittaa annettu ääni. Väestörekisterikeskuksen hallinnoimaa varmennekorttia suositeltiin nettiäänestyksessä käytettäväksi jo edellisessä nettiäänestystä koskevassa esiselvityksessä vuonna 2015.

Oma pohdintansa onkin sitten se, kuinka laajasti korkean tason tunnistusvälineet tulevat olemaan käytössä. Tällä hetkellä korkealla tasolla ovat vain eri organisaatioiden myöntämät varmennekortit, joista yleisin on VRK:n myöntämä henkilökortti. Sähköi-

sen henkilökortin käyttö ei ole kuitenkaan yleistynyt, eikä sitä vaadita missään kansalaisille suunnatuissa palveluissa. Maailmalla on kuitenkin kehitetty erilaisia mobiilitunnistusteknologioita, jotka mahdollisesti tulevaisuudessa soveltuvat myös korkean tason tunnistukseen. Nykyisten Suomessa käytössä olevien mobiilivarmenteiden heikkoutena voisi pitää esimerkiksi operaattorisidonnaisuutta, mutta maailmalla on riippumattomiakin ratkaisuja (mm. MobileConnect). Nämä eivät vielä ole laajemmassa mittakaavassa tulleet käyttöön Suomessa, mutta sähköisten palveluiden käytön yleistyessä tarve helppokäyttöisille vahvoille tunnistusratkaisuille lisääntyy.

Taulukko 2: Tunnistustasojen vertailua

	Korotettu	Korkea
Tunnistusvälineet	Esim. pankkitunnukset	Esim. varmennekortti
Käyttäjät	Käytännössä kaikilla suomalaisilla, joilla tili suomalaisessa pankissa	Sähköinen henkilökortti 690 000 Sos.terv. ammattikortit 235 000 Organisaatiokortit 70 000
Ominaisuudet	Henkilön tunnistus	Henkilön tunnistus ja sähköinen allekirjoitus
Edut	Laajasti käytössä, kaikilla suomalaisilla mahdollisuus saada verkkopankkitunnukset osana peruspankkipalveluita	Tietoturvallinen, varmenteella liikenne voidaan salata äänestystapahtumasta alkaen
Riskit	Tarvitaan erillinen salausmekanismi turvaamaan äänestystapahtuma	Käyttäjäjoukko rajattu, korttien ja lukijoiden hankintakustannukset

Ulkomailla asuvien suomalaisten tunnistaminen

Tällä hetkellä ulkomailla oleskelevien suomalaisten on mahdollista äänestää ulkomaisissa ennakkoäänestyspaikoissa ja tuleva kirjeäänestys tuo mahdollisuuden äänestää postitse. Edustustoja ei kuitenkaan ole kaikissa maissa ja välimatkat ovat pitkiä, joten nettiäänestyksestä on toivottu tähän ratkaisua. Ongelmaksi muodostuu, että nettiäänestys edellyttää kuitenkin vahvaa sähköistä tunnistusta, eikä ulkomailla asuvilla äänioikeutetuilla yleensä ole käytössään suomalaisia sähköisiä tunnistusvälineitä.

Ulkomailla oleskeleva Suomen kansalainen voi hakea sähköistä henkilökorttia edustustosta. Hakijan on oltava henkilökohtaisesti läsnä haettaessa henkilökorttia, eikä hakemusta voida panna vireille sähköisesti.

Kansalaisvarmennetta haetaan henkilökortin hakemisen yhteydessä Suomen edustustolta tai sähköisesti. Haettaessa kansalaisvarmennetta henkilökohtaisesti poliisiviranomaisen luona tai Suomen edustustolta, henkilöllisyys tarkistetaan voimassa olevasta, poliisin myöntämästä henkilöllisyyden osoittavasta asiakirjasta, joita ovat henkilökortti ja passi. Hyväksyttäviä tunnistamisasiakirjoja ovat myös ETA:n jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämä voimassa oleva passi tai henkilökortti ja muun valtion viranomaisen myöntämä voimassa oleva passi.

Peruspankkipalveluita, joihin verkkopankkitunnukset kuuluvat, tarjotaan yhdenvertaisesti ja syrjimättömästi kaikille kuluttaja-asiakkaille, jotka asuvat laillisesti EU- ja ETA-valtioissa. Sähköisen tunnistuspalvelun voi evätä vain, jos asiakkaalla ei esimerkiksi ole henkilötunnusta tai häntä ei ole merkitty väestötietojärjestelmään.

EU-maiden sisällä yksi mahdollinen ratkaisutapa olisi toteuttaa järjestely, jossa esimerkiksi suurlähetystöjen yhteydessä olisi mahdollista todistaa henkilöllisyytensä, rekisteröidä EU:ssa notifioitu tunnistusväline ja liittää se suomalaiseen henkilötunnukseen. Näin nettiäänestyssovellus pystyisi ainakin periaatteessa äänestystilanteessa eIDAS-henkilötietojen avulla hakemaan siihen liitetyn suomalaisen henkilötunnuksen. Tämä ei kuitenkaan ole suunnitteilla.

Sen sijaan henkilöille, jotka asuvat muissa kuin EU/ETA-maissa, ei myönnetä suomalaisia verkkopankkitunnuksia ja tällöin ainoa keino sähköiseen tunnistukseen on sähköinen henkilökortti.

Suomessa asuva ulkomaan kansalainen

Kuntavaaleissa on äänioikeus täysi-ikäisellä kunnan asukkaalla, joka tietyissä tapauksissa voi olla myös ulkomaan kansalainen (ks. Äänioikeus). Lisäksi europarlamenttivaaleissa äänioikeutettuja ovat Suomen kansalaisten lisäksi Suomessa asuvat muiden EU-maiden kansalaiset. Äänioikeutetut henkilöt, jotka ovat Suomessa äänioikeutettuja, voidaan tunnistaa joko verkkopankkitunnuksilla tai sähköisellä henkilökortilla.

Kansalaisvarmenne voidaan myöntää ulkomaalaiselle, jolla on kotikuntalaissa tarkoitettu kotikunta Suomessa, jonka tiedot on talletettu väestötietojärjestelmään ja jonka henkilöllisyys on luotettavasti todennettu. Lisäksi edellytetään, että ulkomaalaisella on voimassa oleva oleskelulupa tai oleskelukortti taikka että hänen oleskeluoikeutensa on rekisteröity.

5 Markkinakartoitus

Markkinakartoituksen tavoitteena oli selvittää, onko markkinoilla tuotteita, jotka täyttäisivät esiselvityksessä tunnistetut vaatimukset ja jotka olisi mahdollista ottaa käyttöön räätälöinnin / jatkokehityksen myötä. Edellinen nettiäänestyksen markkinakartoitus on vuodelta 2013, joten työryhmä päätti tehdä tilannepäivityksen, eikä kokonaan uutta markkinakartoitusta. Tietopyyntö lähetettiin ulkoministeriön kautta niiden Euroopan maiden suurlähetystöihin, joissa tiedetään olleen aktiviteettia nettiäänestyksen suhteen. Osassa maista nettiäänestysjärjestelmä oli aktiivisessa käytössä, osassa on ollut aiemmin käytössä ja joissain järjestelmä on ollut suunnitteilla tai kokeilussa.

5.1 Kansainvälinen vertailu

Viro

Virossa on ollut nettiäänestysmahdollisuus kaikkien äänioikeutettujen käytettävissä vuodesta 2005. Järjestelmä on Cybernetican tuottama ja vuonna 2017 tehtiin suurempi uudistus. Uutta järjestelmää testattiin elokuussa 2017 ja käytettiin ensimmäistä kertaa lokakuun 2017 paikallisvaaleissa. Nettiäänten[8] osuus kaikista äänistä oli näissä vaaleissa 32 %. Kokonaisäänestysprosentti oli 53,4%, joka oli 5% pienempi kuin edellisissä vaaleissa. Viron vaaleissa annettiin ensi kertaa enemmän sähköisiä ääniä kuin täytettiin paperisia vaalilipukkeita. Sähköistä äänestämistä on arveltu kannustimeksi etenkin nuorille. Viron vaaleissa kuitenkin 24 000 äänioikeutetusta 16–17-vuotiaasta vain alle 1800 äänesti sähköisesti. Vaalivilkkauden on määrä selvitä loppuvuonna julkaistavasta Tarton yliopiston tutkimuksesta.[9]

[8] https://kov2017.valimised.ee/osavotu-statistika.html
[9] https://yle.fi/uutiset/3-9891299

Syyskuussa 2017 löydettiin Viron sähköisessä asioinnissa käytetyistä henkilökorteista tietoturvauhka, mutta nettiäänestystä tämä ei estänyt[10]. Marraskuun alussa 2017 Viron hallitus määräsi 760 000 henkilökortin varmenteet suljettavaksi[11] ja korttien varmenteet tulee uusia, jotta niitä voi jatkossa käyttää.

Sveitsi

Sveitsin 26 kantonista kuudessa on käytössä nettiäänestysjärjestemä. Näistä kolme tarjoaa netissä äänestämisen mahdollisuutta vain ulkomailla asuville sveitsiläisille. Basel mahdollistaa äänestämisen ulkomailla asuvien lisäksi vammaisille äänestäjille. Geneven ja Neuchâtelin kantoneissa myös osa asukkaista voi äänestää internetin välityksellä.

Kantonit vastaavat itse äänestysjärjestelmistään ja mikäli halutaan käyttää järjestelmää myös liittovaltion kansanäänestyksissä, se tulee hyväksyttää liittovaltion hallinnolla määrättyjen kriteerien perusteella. Tällä hetkellä käytössä on Geneven kantonin (CHVote) ja Swiss Postin (Scytl) kehittämät järjestelmät. CHVoten käyttöönottoa valmistellaan useammassa kantonissa, ja pidemmän ajan tavoitteena on tarjota internetäänestysmahdollisuutta kaikille. Uusimman (2017) tutkimuksen mukaan internetäänestys ei ole lisännyt äänestysaktiivisuutta[12] Sveitsissä.

Norja

Norjassa oli nettiäänestyskokeilu vuosina 2012 ja 2013, jolloin käytössä oli Scytlin toteuttama nettiäänestysjärjestelmä. Nettiäänestysmahdollisuutta tarjottiin 10 kunnassa vuonna 2012 ja 12 kunnassa vuonna 2013 ja kokeiluun oltiin tyytyväisiä. Kokeilun myötä vaalisalaisuuden merkitys nousi kuitenkin niin voimakkaasti keskusteluun, että lopulta tehtiin poliittinen päätös, ettei nettiäänestystä jatketa, koska äänestys ei tapahdu vaaliviranomaisen valvonnassa. Poliittista yksimielisyyttä vaalitavoista pidetään niin tärkeänä, ettei nettiäänestyksen käyttöönotto ole tällä hetkellä suunnitelmissa.

Ranska

Ranskassa pilotoitiin internetäänestystä kunnallisvaaleissa vuonna 2002. Internetäänestystä (toimittajana Scytl) käytettiin 2003–2009 kirjeäänestyksen rinnalla ulko-

[10] National Electoral Committee: e-voting will take place [https://www.valimised.ee/en/news/national-electoral-committee-e-voting-will-take-place]
[11] Id.ee http://id.ee/index.php?id=30519&read=38341
[12] Micha Germann, Uwe Serdült. Internet voting and turnout: Evidence from Switzerland. 2017.

ranskalaisten parlamentin vaaleissa ja tämän jälkeen ulkoranskalaisille 2012 parlamenttivaaleissa. Ranskassa asuville internetäänestys ei siis ole ollut käytössä kunnallisvaalipilotin jälkeen. Maaliskuussa 2017 Ranska ilmoitti, että internetäänestysmahdollisuus poistetaan käytöstä Ranskan puolustuksesta ja turvallisuudesta vastaavan sihteeristön suosituksesta. Lokakuussa 2017 presidentti Macron mainitsi puheessaan[13], että nettiäänestys voitaisiin mahdollisesti jossain vaiheessa ottaa takaisin käyttöön.

Ruotsi

Ruotsissa selvitettiin hallituksen toimeksiannosta internetäänestyksen käyttöönottoa ja 2013 julkaistussa loppuraportissa komitea ehdotti selvityksen tekemistä, jotta internetäänestystä voitaisiin kokeilla vuoden 2018 vaaleissa. Maaliskuussa 2017 kuitenkin vahvistettiin, ettei Ruotsi aio valmistella internetäänestystä vuoden 2018 vaaleihin. Jos sähköistä äänestystä kokeiltaisiin, se tapahtuisi aikaisintaan 2022 ja äänestys tapahtuisi valvottuna vaalipaikalla.

Liettua

Liettuassa ei ole internetäänestystä käytössä tällä hetkellä, mutta vuoden 2017 hallitusohjelmaan on kirjattu internetäänestyksen käyttöönotto tietoturvan ja vaalisalaisuuden varmistaen. Liettuan oikeusministeriö valmistelee lainsäädäntöä, joka mahdollistaisi internetäänestyksen käyttöönoton. Suurimpana haasteena tunnistetaan kansalaisten luottamuksen saavuttaminen. Järjestelmän tulisi olla auditoitavissa ja vapaasti testattavissa ennen käyttöönottoa.

Islanti

Islannissa on tarjottu vuosina 2015–2016 kuudelle kunnalle mahdollisuutta kokeilla internetäänestystä kunnallisessa kansanäänestyksessä, mutta toistaiseksi vain kaksi kuntaa on hyödyntänyt tätä mahdollisuutta. Kyseessä on Scytlin tuote ja kokeilu on kunnille maksuton. Ulkomailla asuvat ja vammaiset katsotaan ryhmiksi, jotka hyötyisivät nettiäänestysmahdollisuudesta.

Yleistä

[13] http://www.elysee.fr/declarations/article/discours-du-president-de-la-republique-emmanuel-macron-a-l-occasion-de-la-27-session-pleniere-de-l-assemblee-des-francais-de-l-etranger/

Merkittävää kokonaisäänestysprosentin nousua ei ole nettiäänestyksen myötä tapahtunut, mutta saaduissa vastauksissa nousivat esille ulkomailla asuvien äänestysprosentin nousu ja vammaisten äänestämisen helpottaminen. Järjestelmän ja prosessin avoimuutta pidetään keskeisenä luottamuksen kannalta, joten järjestelmän auditointimahdollisuus katsotaan tärkeäksi. Luottamuksen kannalta tärkeäksi on katsottu, että äänestäjä pystyisi varmistamaan oman äänensä perille menon (individual verifiability) ja että jokaisen äänen olemassaolo voidaan yleisesti varmistaa (universal verifiability).

Riskeiksi kyselyyn vastanneet maat nimeävät luottamuksen, kyberuhat, tietoturvallisuuden, vaalisalaisuuden, vaaleihin vaikuttamisen ja korkeat kustannukset. Vaikeammin mitattavana ja hallittavana riskinä nousee esiin maineriski. Sveitsin vastauksessa nostetaan esille esimerkki, jossa kansalainen väitti hakkeroineensa nettiäänestysjärjestelmän, vaikka kyse oli ollut yksinkertaistetusta kopiosta, jonka suojaus oli heikompi. Maineriskit onkin Sveitsissä otettu huomioon kaikissa riskianalyyseissa ja koko prosessissa alkaen kehityksestä ja käyttäjäkokemuksen suunnittelusta lainsäädäntöön ja julkiseen viestintään.

Ahvenanmaalla on selvitetty nettiäänestyksen käyttöönottoa ja valmisteltu tämän maakunnan omissa vaaleissa mahdollistavaa lakia. Tarkoitus on nettiäänestyksen avulla helpottaa Ahvenanmaan ulkopuolella asuvien äänestämistä. Vaihtoehtoina on selvitetty hankintaa valmistuotteena tai palveluna, mutta omaan kehitykseen ei ole resursseja.

5.2 Käytössä olevat ratkaisut

Nettiäänestysjärjestelmistä järjestettiin vuonna 2013 tekninen vuoropuhelu, johon osallistui 8 teknistä toimittajaa. Hankintailmoitus oli avoin ja vuoropuheluun osallistui tuolloin myös yrityksiä, joilla ei ollut valmista tuotetta, mutta jotka olivat kiinnostuneita kehittämään sellaisen. Tässä esiselvityksessä työryhmä on rajannut edellisen selvityksen ja kansainvälisen vertailun päivityksen perusteella tietopyynnön toimittajiin, joilla on tällä hetkellä Euroopassa valtakunnallisissa vaaleissa käytettävä nettiäänestysjärjestelmä. Näitä ovat virolainen Cybernetica ja espanjalainen Scytl. Molemmat toimittajat kutsuttiin tapaamiseen, jossa keskusteltiin etukäteen valmistellun asialistan puitteissa. Tämän lisäksi molemmille lähetettiin toteutustekniikkaa ja tietoturvaa käsittelevä kysymyslista, johon pyydettiin toimittamaan vastaukset tapaamisen jälkeen.

Scytl tarjoaa kaupallista tuotetta, joka käytännössä räätälöidään aina käyttöönottavan maan vaalijärjestelmään ja infrastruktuuriin sopivaksi. Lähdekoodin avaaminen julkiseksi onnistuu ainakin osin ja näin toimittiin esimerkiksi Norjassa, kun järjestelmä oli

siellä käytössä. Tuotteen hyödyntäminen on kuitenkin mahdollista vain niin, että Scytl toimii tuotteen kaupallisena järjestelmätoimittajana.

Cybernetican toteutuksen lähdekoodi on julkisesti nähtävillä, mutta lisenssi ei mahdollista uudelleenkäyttöä ja jatkokehitystä. Viron valtio omistaa tuotteen, joten yhteistyö X-Roadin[14] malliin voisi olla eräs selvitettävä toimintatapa.

Toimittajien vastauksista tehtiin yhteenveto ja analyysi, jossa vertailtiin vastauksia lähetettyihin kysymyksiin. Saatujen vastausten perusteella ei kumpaakaan toimittajaa ole perusteltua sulkea tässä vaiheessa pois mahdollisena nettiäänestysjärjestelmän toimittajana Suomen yleisiin vaaleihin. Esiselvityksen riskikartoituksessa esiin tuotuja merkittävimpiä riskejä ei kuitenkaan voida hallita täysin kummankaan valmistajan tuotteilla. Todennäköisesti toteutukseen jää merkittäviä jäännösriskejä, jotka on hyväksyttävä ennen nettiäänestysjärjestelmän toteutuspäätöstä.

Tiettyjen vaaleihin kohdistuvien periaatteellisten vaatimusten osalta voidaan joutua tekemään päätös luopua joistakin tarpeista, jotta jonkin toisen vaatimuksen toteuttaminen tulisi mahdolliseksi. Nämä päätökset edellyttävät poliittista harkintaa.

Toimittajien suhtautumisessa tietoturvaan ohjelmistokehitysprosessissa on toimittajakohtaisia eroja, jotka voivat vaikuttaa tuotteen turvallisuuteen. Varsinaisessa hankintaprosessissa on varattava riittävästi aikaa tuotteiden turvallisuusominaisuuksien auditointiin.

Toimittajien ratkaisut koskevat äänestämisen järjestämisen osaongelmia, eivätkä itsessään ole valmiita avaimet käteen -ratkaisuja. Kokonaistoteutukseen liittyy toimittajien ulkopuolelle rajaamia järjestelmäkokonaisuuksia, kuten äänestäjien tunnistamiseen käytettävät palvelut.

Ainoastaan toimittajien ratkaisuilla äänten eheä toimitus äänestäjältä vahvistettuun tulokseen (päästä päähän) ei toteudu. Molemmat järjestelmät asennettaisiin asiakkaan palvelimille ja asiakkaalla olisi vähintään osavastuu niiden operoinnista. Kokonaisvastuu auditoinnin ja monitoroinnin toteutuksesta, seurannasta ja hälytyksistä on siis asiakkaalla, koska tuote on vain osa kokonaisuutta, johon kuuluu esimerkiksi käyttöprosessi sekä tekninen ympäristö, johon tuote asennetaan. Dokumentaation ja lähdekoodin avoimuus ei ollut myöskään itsestään selvää vaan neuvottelukysymys.

[14] https://esuomi.fi/palveluvaylan-yhteistyomalli-viron-kanssa/

5.3 Puitesopimukset ja avoin lähdekoodi

Esiselvityksessä ei ole tullut esille sovellettavissa olevia puitesopimuksia, joilla nettiäänestyssovellus olisi suoraan mahdollista toteuttaa tai hankkia. Ohjelmistokehitystä sen sijaan voidaan hankkia Hanselin puitejärjestelyiden kautta.

Avoimena lähdekoodina julkaistuja nettiäänestyssovelluksia on joitain (mm. Helios), mutta useimpia ei ole tarkoitettu valtakunnallisiin vaaleihin. Sveitsin Geneven kantonissa käytetyn CHVoten lähdekoodi on avointa lähdekoodia ja hankintavaiheessa voi myös tätä ratkaisua tarkastella lähemmin. Suoraan ei tämä äänestyssovellus kuitenkaan täytä tunnistettuja vaatimuksia mm. päästä päähän salauksen puutteen vuoksi.

5.4 Hankintavaihtoehdot

Tässä esiselvityksessä on pyritty tunnistamaan vaatimukset ja reunaehdot nettiäänestysjärjestelmän onnistuneelle hankinnalle. Esiselvitys ei ole itsessään osa hankintamenettelyprosessia. Nettiäänestysjärjestelmän omistajana olisi oikeusministeriö ja sen alainen Oikeusrekisterikeskus vastaisi käytännössä järjestelmän hankinnasta, sopimushallinnasta ja ylläpidosta.

Ohjelmistotuotteen hankinnassa on seuraavia vaihtoehtoja:

1. Valmistuotteen ostaminen
    - Räätälöinti
2. Ohjelmiston ostaminen palveluna
3. Tuotteen kehittäminen itse
    - Avoin
    - Suljettu

Usein yksinkertaisin ja helpoin malli on valmistuotteen tai palvelun hankkiminen. Mahdollinen räätälöinti voidaan hankkia ohjelmistotoimittajalta tai joissain tapauksissa erilliseltä toimittajalta. Ohjelmistotoimittaja tuntee tuotteensa hyvin, joten se on usein nopein ja tehokkain tapa tehdä halutut muutokset ohjelmistoon. Hankinnassa tulee kuitenkin kiinnittää huomiota nettiäänestyssovelluksen omistajuuteen, sijoitukseen ja immateriaalioikeuksiin. Järjestelmän toiminnan jatkuvuuden takaamiseksi sovelluksen tulee jäädä oikeusministeriölle/Oikeusrekisterikeskukselle, kun sopimus teknisen toimittajan kanssa päättyy. Näin siis palveluna (Saas) hankittavat sovellukset eivät tule kyseeseen. Saas ei myöskään tuo säästöjä tilanteissa, joissa palveluna hankittavalla

ohjelmistolla ei ole useita asiakkaita, joiden järjestelmiä voidaan tuottaa samalla infrastruktuurilla.

Nettiäänestysjärjestelmän lähdekoodin tulee olla julkinen, mutta lähdekoodia ei tarvitse välttämättä avata vapaasti hyödynnettäväksi (open source). Lähdekoodin julkisuus on tarpeen tietoturvan varmistamiseksi ja luottamuksen lisäämiseksi. Koodin vapaa hyödynnettävyys takaisi sen, että järjestelmää voidaan ylläpitää ja kehittää edelleen senkin jälkeen, kun sopimus toimittajan kanssa on päättynyt, mutta tämä voidaan varmistaa myös muilla sopimuksellisilla keinoilla. Yrityksissä on eroja suhtautumisessa ohjelmistotuotteen avoimuuteen, joten jo ennen hankintaprosessiin lähtemistä tulee olla selvillä tilaajan vaatimuksista koodin julkisuuden ja hyödynnettävyyden suhteen.

Julkisissa ohjelmistohankkeissa on riskialtteimmaksi todettu tuotteen kehittäminen alusta alkaen suljetulla lähdekoodilla. Tämä voi olla erittäin hidasta ja kallista, koska nettiäänestysjärjestelmän kehittäminen vaatii pitkälle erikoistunutta äänestysjärjestelmien, tietoturvan ja kryptologian erityisosaamista. On järkevämpää hyödyntää pohjana nettiäänestysjärjestelmiä tarjoavien yritysten kokemuksen kautta kertynyttä osaamista, ja jatkaa jatkokehitystä esiselvityksessä tunnistettujen lisävaatimusten perusteella. Tässä mallissa hankkeen toteuttamiseen liittyvät aikataulu- ja laaturiskit olisivat parhaiten hallittavissa.

Markkinakartoituksen perusteella on olemassa tuotteita, jotka voisivat toimia järjestelmän ytimenä, mutta vaatisivat jatkokehitystä. Perinteisen räätälöinnin lisäksi tässä voisi toimia myös malli, jossa hankitaan pohjalle tuote ja hankitaan erikseen jatkokehitysosaamista. Jatkokehitys voidaan tehdä virkatyönä palkkaamalla osaajia Oikeusrekisterikeskukseen, hankkimalla puhtaasti ohjelmistokehitystä tai näiden yhdistelmänä. Projektin vetovastuu tulee kuitenkin olla Oikeusrekisterikeskuksessa, joten sinne tulee rekrytoida riittävää teknistä osaamista ja samalla varmistaa, että kehitysprojektin aikana ylläpidosta vastaaville kertyy vankka osaaminen tuotteesta.

Ohjelmistoprojektissa on neljä tekijää, jotka vaikuttavat siihen, millä mallilla ohjelmisto kannattaa toteuttaa. Nämä ovat hinta, laajuus, aikataulu ja laatu. Käytännössä kaikkia ei voi samanaikaisesti priorisoida ja suunnittelussa tuleekin tehdä arviointia siitä, mikä on juuri kyseisessä ohjelmistoprojektissa tärkeintä. Nettiäänestysjärjestelmässä tietoturvakriittisyyden ja käytettävyysvaatimusten vuoksi toteutuksen laatu ja ominaisuudet nousevat muiden edelle. Kustannusten karkaaminen on laatua varmistaessa myös merkittävä riski, jota ei voi olla ottamatta huomioon julkishallinnon hankkeessa. Laajuudessa ja aikataulussa voisi sen sijaan joustaa. Toiminnallisuuksia voidaan supistaa tai toteuttaa ensi vaiheessa yksinkertaistettu tai rajattu järjestelmä ja lisätä ominaisuuksia/laajuutta, kun perusta on testattu toimintavarmaksi. Projektin suunnittelussa ja hankintasopimuksissa tulee ottaa huomioon se, että projektilla on aikataululliset

raamit, mutta niistä ei pidetä kiinni laadun kustannuksella. Toisin sanoen nettiäänestysjärjestelmää ei voi ottaa käyttöön ennen kuin voidaan olla täysin varmoja siitä, että sitä on testattu riittävän paljon, riittävällä laajuudella ja kaikki todetut haasteet on saatu korjattua ja testattu. Ketterällä kehitysmallilla voidaan mahdollistaa käyttäjätestaus koko kehitysprosessin aikana prototyypistä alkaen.

Esiselvityksessä on tuotettu alustava vaatimusmäärittely, jota tulee vielä tarkentaa ennen hankintaprosessiin lähtemistä, mutta ketterässä ohjelmistoprojektissa ei liian tarkkaa vaatimusmäärittelyä tule tehdä, koska muuten lopputulos voi vaarantua jo ennen projektin alkamista. Ennen hankinnan käynnistämistä oikeusministeriön/ Oikeusrekisterikeskuksen pitää varmistaa riittävä osaaminen kilpailutusprosessin läpiviemiseksi palkkaamalla riittävän pätevää teknistä projektinjohtoa. Useissa vaikeuksiin ajautuneissa julkisissa hankkeissa ongelmana on ollut järjestelmän hankkijan oman kompetenssin ja resurssien puute. Erityisesti ketterässä ohjelmistoprojektissa tuoteomistajan osaamisen merkitys korostuu.

Tietoturvakriittisten osien (protokolla, salaus) toteutuksen hankinnassa tulisi käyttää POC:ia (Proof of Concept), jolloin voidaan varmistua, että hankittava osaaminen ja menetelmät ovat vaaditulla tasolla.

Nettiäänestysjärjestelmän ennakoitu arvo ylittää selvästi hankintalain (1397/2016) 26 §:ssä tarkoitetun EU-kynnysarvon. Se tarkoittaa, että hankintaan voivat osallistua toimittajat, jotka toimivat EU:n alueella. Nettiäänestysjärjestelmä olisi pitkän elinkaaren järjestelmä. Niinpä järjestelmän teknologiavalinnoissa ja jatkokehityksessä on syytä ottaa huomioon teknologian nopean kehityksen vaikutukset. Kun määritellään hankinnan ennakoitua arvoa, kyseeseen tulevat järjestelmän hankintakustannukset, kehityskustannukset sekä järjestelmän elinkaarikustannukset ja vaalikohtaiset kustannukset.

Koska valtiollisissa vaaleissa käytettäviä nettiäänestysjärjestelmiä on markkinoilla markkinakartoituksen perusteella vähän, on mahdollista, että jotkut vaatimukset voivat sulkea merkittävän määrän tarjoajia ulos kilpailusta. Esimerkiksi päätelaitteesta riippumatonta äänestämisen turvallisuutta tarjoaa vain yksi toimittaja, kun taas toinen ratkaisu perustuu päätelaitteen turvallisuuteen. KHO on ratkaisussaan KHO:2017:152[15] linjannut, että julkisessa hankinnassa voidaan painottaa korkeaa laatua ja tarvittaessa edellyttää ominaisuuksia, jotka edustavat teknisen kehityksen huippua, vaikka niitä ei vielä olisi laajasti markkinoilla.

[15] http://www.kho.fi/fi/index/paatoksia/vuosikirjapaatokset/vuosikirjapaatos/1506942292484.html

Hankintavaihtoehtoina ovat avoimen hankinnan lisäksi neuvottelumenettely, kilpailullinen neuvottelumenettely ja innovaatiokumppanuus. Kaksi jälkimmäistä voidaan valita suoraan, jos perusteet täyttyvät, mutta myös jos avoimessa hankintamenettelyssä päädytään tilanteeseen, jossa avoimessa hankintakilpailussa ei saada tarjousta sopivasta nettiäänestysjärjestelmästä, samaa hankintaa voidaan jatkaa neuvottelumenettelynä. Hankintalain 34 §:n 3 momentin mukaan hankintayksikkö voi valita neuvottelumenettelyn, jos avoimessa tai rajoitetussa menettelyssä on saatu vain tarjouksia, jotka eivät vastaa tarjouspyyntöä, tai jos tarjouksia ei voida hyväksyä. Uutta hankintailmoitusta ei tarvitse julkaista, jos neuvottelumenettelyyn otetaan mukaan kaikki ne tarjoajat, jotka täyttävät asetetut vähimmäisedellytykset ja jotka ovat edeltävässä menettelyssä tehneet tarjousmenettelyn muotovaatimusten mukaisen tarjouksen.

Neuvottelumenettelyissä tulee huolehtia tasapuolisuudesta ja laadusta erityisesti, kun lähdetään neuvottelemaan vaatimuksista. On tunnistettava ehdottomat vaatimukset, eriteltävä jo ennen hankintaprosessia ne, joissa voidaan joustaa tarvittaessa. Ehdottomista vaatimuksista ei neuvotella, mikä tulee ottaa huomioon jo hankintadokumentteja ja vaatimusmäärittelyä laadittaessa.

Kilpailullinen neuvottelumenettely on taas selkeästi kaksivaiheinen. Ensimmäisessä vaiheessa etsitään haluttu ratkaisu ja toisessa vaiheessa pyydetään tähän ratkaisumalliin perustuvat tarjoukset. Neuvottelumenettelyssä tarjouksia saatetaan pyytää suhteessa aikaisemmassa vaiheessa kuin kilpailullisessa neuvottelumenettelyssä. (Tekes)[16] Kaksivaiheisuudessa on etunsa, koska tällöin on mahdollista tarkentaa hankittavaa ratkaisua. Neuvottelumenettelyt vaativat kuitenkin hankintaorganisaatiolta aikaa ja resursseja huomattavasti enemmän paperilla tehtävään hankintaan verrattuna.

Koska Suomen valtiollisiin vaaleihin hankittava nettiäänestysjärjestelmä olisi uusi innovaatio, myös hankintalain 38 §:ssä tarkoitettu innovaatiokumppanuus voisi tulla kyseeseen. Innovaatiokumppanuutta voidaan käyttää tyypillisesti silloin, kun markkinoilla on hankintayksikön tarpeita lähellä olevia ratkaisuja, jotka eivät kuitenkaan täytä hankintayksikön tarpeita esimerkiksi laadun tason, asiakkaiden tarpeiden tai kehitysasteen osalta. Innovaatiokumppanuuden riskeinä voivat olla sen korkea hinta ja se, että se edellyttää tilaajapuolelta avointa kilpailua enemmän joustavuutta, resursseja ja osaamista.

[16] https://www.tekes.fi/globalassets/julkaisut/tyokirja_kilpailullisen_neuvottelumenettelyn_toteuttamiselle.pdf

Käytettävä hankintamenettely on tarkoituksenmukaisinta valita vasta, kun nettiäänestysjärjestelmän hankinta on päätetty käynnistää ja tarvittavat periaatteelliset linjaukset on tehty. Tämän jälkeen tarkennetaan vaatimusmäärittelyä ja luodaan käyttötapaukset. Tässä yhteydessä tehdään hankintamenettelyn valinta ja tarvittaessa sitä ennen tarkentava tekninen vuoropuhelu.

6 Tietoturvallisuuden varmistaminen

6.1 Riskien arviointi

Osana esiselvitystä F-Secure toteutti oikeusministeriön toimeksiannosta tietoturvariskien kartoituksen. Työ perustui olemassa olevien dokumenttien katselmointiin sekä kahteen työpajaan, joihin kutsuttiin oikeusministeriön valitsemien sidosryhmien edustajat. Toimeksiannon alainen työskentely ajoittui huhti- ja toukokuulle 2017. Riskikartoitusta laadittaessa ei ollut tiedossa, millainen toteutettava äänestysjärjestelmä olisi, joten käsittelytavaksi valittiin taso, jossa teknologiasidonnaiset kysymykset eivät olennaisesti vaikuta.

Tietoturvariskien kartoituksessa pyrittiin tunnistamaan eri uhkatoimijat, riskien vaikutukset ja kuinka tunnistettuja riskejä voidaan pyrkiä hallitsemaan. Riskienhallinnan toimenpiteistä johdatettiin vaatimuksia nettiäänestysjärjestelmälle. Nämä on kirjattu alustavaan vaatimusmäärittelyyn.

Markkinakartoituksen perusteella riskejä ei voi täysin poistaa tai välttää nettiäänestysjärjestelmässä. Tästä johtuen ne on hyväksyttävä vähintään osittain. Hyväksyntäpäätöstä tehtäessä on tunnettava, millaisia vaikutuksia riskien toteutumisella voi olla.

Riskijäännöksen todennäköisyyden ja vaikutuksen täsmällinen arviointi on hankalaa ilman tietoja järjestelmän hankinta- ja toteutustavasta. Tästä huolimatta on mahdollista kuvailla näiden vakavien häiriöiden vaikutuksia erilaisten operatiivisten kustannustekijöiden näkökulmasta.

Keskeisimmiksi riskeiksi selvityksessä tunnistettiin vaalituloksen laaja manipulointi, vaalien häirintä palvelunestohyökkäyksillä ja vaalisalaisuuden laajamittainen murtuminen.

Vaalituloksen laaja manipulointi

Nettiäänestysjärjestelmä luo uudenlaisen mahdollisuuden manipuloida yleisten vaalien tulosta. Nykyisissä manuaalisissa äänestystavoissa ääntenlasku on hajautettu, minkä johdosta vaalituloksen merkittävä manipulointi edellyttäisi laajaa laskentaan osallistuvien salaliittoa. Tällöin äänestyslippuja hävitettäisiin tai muokattaisiin huomattavia määriä, jotta tarkistuslaskennassa tulos ei muuttuisi. Nettiäänestyksessä tulosten laskenta ja julkaisu tapahtuisi keskitetysti tietojärjestelmässä, jonka toimintaa valvoisi huomattavasti pienempi henkilömäärä. Nettiäänestyksen ollessa käytössä muiden vaihtoehtojen rinnalla vastaavan vaikutuksen saamiseen voi riittää tietojärjestelmän tietosisällön muokkaaminen niin, että annettuja ääniä poistetaan tai siirretään toisille ehdokkaille. Manipuloinnin mahdollisuudet ovat sitä laajemmat, mitä suurempi osuus äänistä annetaan netissä.

Suomessa vaalitulos vahvistetaan aina ääntenlaskennan päätyttyä. Vahvistetun tuloksen perusteella vaaleissa valitut henkilöt saavat asemansa mukaiset valtuudet. Näin tapahtuu myös silloin, kun vaaleissa epäillään vilppiä. Vahvistetusta tuloksesta on mahdollista valittaa[17], ja vaalit voidaan uusia oikeuden päätöksellä, mikäli näyttöä epäselvyyksistä voidaan osoittaa. Tuloksen vahvistamisesta voi kulua kuitenkin kuukausia tai vuosia siihen, että riittävä tietotekninen näyttö on kerätty ja käsitelty eri oikeusasteissa, ja uudet vaalit järjestetty. Erikoinen tai odotuksista poikkeava vaalitulos ei itsessään ole näyttö vilpistä. Äänestyslippuja käytettäessä suuri osa epäilyksistä voidaan selvittää sillä, että tulosta epäilevä tai riippumaton taho laskee äänet uudelleen. Useimmissa vaalisalaisuuden takaavissa nettiäänestysjärjestelmissä ei ole mahdollista tehdä uudelleenlaskentaa samassa merkityksessä.

Ennen uusien vaalien järjestämistä vaaleissa valitut voivat käyttää asemansa mukaista valtaa. Kunnallisella tasolla valtuutetut voivat tehdä päätöksiä, joilla voi aiheutua merkittäviä taloudellisia hyötyjä tai haittoja joillekin tahoille. Eduskuntaan valitut kansanedustajat voivat säätää lakeja ja äärimmäisessä tapauksessa muuttaa perustuslakia kiireellisen säätämisjärjestyksen mukaisesti. Tästä johtuen, vaalituloksen laajamittainen manipulointi voi onnistuessaan olla yhteiskunnan vakauden näkökulmasta äärimmäisen vahingollinen tapahtuma.

Nettiäänestysjärjestelmän tietosisällön manipulointi voi olla mahdollista uhkatoimijalle, joka on riittävän motivoitunut vaikuttamaan yleisten vaalien tulokseen ja jolla on riittävä keinovalikoima toimenpiteen toteuttamiseksi. Motivaatioita ja keinoja käsitellään tarkemmin riskikartoituksessa. Nämä tunnistetut keinot avaavat mahdollisuuden manipuloida yleisten vaalien tuloksia.

[17] Presidentinvaalissa valitusoikeutta ei ole.

Manipuloinnin tapahtuessa ylimääräisiä operatiivisia kustannustekijöitä muodostuu vähintään seuraavista syistä:

- Tietoteknisen tutkinnan suorittaminen kestää viikoista kuukausiin. Osa työstä tehdään ostopalveluna ja se maksaa todennäköisesti satoja tuhansia euroja.
- Muun tutkintaa tukevan näytön kerääminen vie poliisin resursseja.
- Vaalien mitätöinnin käsittely eri oikeusasteissa kuormittaa oikeuslaitosta.
- Manipuloiduissa vaaleissa valittujen tekemien päätösten oikeudellinen asema joudutaan arvioimaan uudelleen, joskin vasta uusittavissa vaaleissa valitun uuden toimielimen toimesta. Riippuen tehtyjen päätösten sisällöstä ja määrästä, kyse voi olla huomattavasta hallinnon virkamiehiä ja oikeuslaitosta kuormittavasta toimenpiteestä.
- Hallinnollisten päätösten valmistelu ja päätöksenteko hidastuu tai pysähtyy, kun päätöksentekijöiden asema on epäselvä. Tämä estää ja ruuhkauttaa eritasoisten asioiden etenemisen.
- Vaalit joudutaan järjestämään uudelleen. Valtion ja kuntien kustannukset ovat kymmeniä miljoonia euroja. Ehdokkaat joutuvat uusimaan kampanjansa, joka kuormittaa ehdokkaiden ja puolueiden taloutta. Pohdittavaksi tulevat myös vahingonkorvausasiat.
- Oikeusministeriö käyttää ylimääräisiä voimavaroja uusittavien vaalien luotettavuuden varmistamiseksi. Tämä lähes väistämättä tarkoittaa myös sitä, että nettiäänestysjärjestelmää ei enää käytetä, ja investoinnista ei saada siitä kaavailtua hyötyä.

Kokonaisuutena kuvailtu tapahtuma maksaa yhteiskunnalle erilaisina vaikutuksina kymmeniä miljoonia euroa. Riskin toteutumisen todennäköiset vaikutukset ovat moninkertaiset nettiäänestysjärjestelmästä saavutettavaan hyötyyn nähden.

Vaalien häirintä palvelunestohyökkäyksillä

Vaalien häirintä tietoteknisillä keinoilla muodostaa uudenlaisen riskin demokraattiseen vaalijärjestelmään. Kaikki internetiin liitetyt palvelut altistuvat jollakin tasolla palvelunestohyökkäyksille. Näillä hyökkäyksillä tarkoitetaan tilannetta, jossa uhkatoimija synnyttää ylimääräistä tietoliikennettä, muuta kuormitusta tai yhteyksien katkeamisen ja palvelun luvalliset käyttäjät eivät voi ottaa yhteyttä palvelun toimintoihin.

Palvelunestohyökkäys on ongelmallinen yhtäläisen äänioikeuden toteutumisen näkökulmasta. Yhtäläisellä äänioikeudella tarkoitetaan sitä, että jokaisella äänioikeutetulla on yhtäläinen oikeus vaikuttaa vaalin tulokseen. Nettiäänestyksen toteutuessa voidaan ajatella, että äänioikeutetulla on oikeus antaa äänensä nettiäänestysjärjestel-

mällä. Mikäli tämä ei toteudu palvelunestohyökkäyksen tai muun häiriön johdosta, ei äänioikeutetulla välttämättä ole mahdollisuutta antaa ääntä muulla äänestystavalla.

Palvelunestohyökkäysten toteuttaminen ei ole kallista ja niitä voi ostaa palveluna. Hyökkäysten torjunta on vaikeaa ja perustuu yleensä joko palveluun kohdistuvan tietoliikenteen tilapäiseen rajoittamiseen, esimerkiksi Suomen rajojen ulkopuolelta tulevan tietoliikenteen perille toimittamisen estämiseen, tai itse palvelun hajauttamiseen lukuisiin, yleensä eri maissa sijaitseviin palveluympäristöihin.

Riskin vaikutuksiin voidaan olennaisesti vaikuttaa varautumalla ennakolta lainsäädännössä tahallisiin palvelunestoihin ja muihin sellaisiin IT-häiriötilanteisiin, jotka voivat estää nettiäänestysjärjestelmän hyödyntämisen. Äänestysmahdollisuus paperiäänellä ennakkoäänestysaikana ja varsinaisena vaalipäivänä voi osaltaan turvata yhtäläisen osallistumisoikeuden.

Mikäli palvelunestot tai IT-häiriöt voivat johtaa vaalien uusimiseen, muodostuu ylimääräisiä operatiivisia kustannustekijöitä vähintään seuraavista syistä:

- Vaalien mitätöinnin käsittely eri oikeusasteissa kuormittaa oikeuslaitosta.
- Vaalit joudutaan järjestämään uudelleen. Valtion ja kuntien kustannukset ovat kymmeniä miljoonia euroja. Ehdokkaat joutuvat uusimaan kampanjansa, mikä kuormittaa ehdokkaiden ja puolueiden taloutta.
- Oikeusministeriö käyttää ylimääräisiä voimavaroja uusittavien vaalien luotettavuuden varmistamiseksi. Tämä lähes väistämättä tarkoittaa myös sitä, että nettiäänestysjärjestelmää ei enää käytetä, ja investoinnista ei saada siitä kaavailtua hyötyä.

Kokonaisuutena kuvailtu tapahtuma voi maksaa yhteiskunnalle erilaisina vaikutuksina kymmeniä miljoonia euroa. Riskin toteutumisen todennäköiset vaikutukset ovat moninkertaiset nettiäänestysjärjestelmästä saavutettavaan hyötyyn nähden.

Vaalisalaisuuden laajamittainen murtuminen

Saatavilla olevien nettiäänestysjärjestelmien tekninen toteutustapa jättää mahdollisuuden vaalisalaisuuden murtamiselle. Huolimatta käytössä olevista salausalgoritmeista, nettiäänestystapahtuman eri vaiheissa syntyy riittävä määrä tietoa, joita yhdistelemällä on mahdollista selvittää kunkin äänestäjän antama ääni. Tältä osin nettiäänestysjärjestelmissä ei saavuteta vaalipäivänä tapahtuvan äänestämisen tasoista vaalisalaisuutta.

Myös muissa äänestystavoissa on teoriassa mahdollista selvittää yksittäisten äänestäjien antamia ääniä. Ennakko-, koti-, ja kirjeäänestyksessä tieto äänestäjästä sekä äänestyslippu ovat joissakin prosessin vaiheissa yhdistettävissä toisiinsa. Vaaliviranomaiset kuitenkin käsittelevät asiakirjoja virkavastuulla. Nettiäänestys on äänestystavoista ainoa, jossa yhden keskitetyn järjestelmän turvallisuusongelma voi johtaa siihen, että kaikkien kyseistä äänestystapaa hyödyntäneiden äänet paljastuvat

Lisäksi nettiäänestys tapahtuu käyttäjän omalla laitteella, jonka turvatasoa ei ole mahdollista valvoa. Niinpä äänestystapahtuman tekninen vakoileminen voisi olla mahdollista. Suurin vahinko syntyy, jos haittaohjelma onnistuu vakoilemaan suurta määrää äänestäjiä.

Riskin toteutumisesta aiheutuvia kustannuksia on vaikea arvioida, sillä ne eivät kohdistu keskitetysti. Luultavasti äänien paljastuminen aiheuttaisi yksilötason inhimillistä kärsimystä ja yhteiskunnallista epävakautta tavoilla, joita ei Suomessa nykyisen vaalisalaisuuden ja äänestämisen vapauden piirissä voida täysin ennakoida. Esimerkiksi erilaisissa etupiireissä luultavasti pyrittäisiin tällaisen aineiston tullessa julki selvittämään tarkoin, miten omat jäsenet äänestivät.

Riskin hyväksymisen näkökulmasta päätöksentekijän on arvioitava se, mikä arvo nykyisen tasoisella vaalisalaisuudella on. Nettiäänestäminen lisää mahdollisuuksia annettujen äänien paljastumiseen.

Oman erityispiirteensä vaalisalaisuuden säilymiseen muodostaa se, että salausalgoritmeilla on rajallinen elinkaari. Nettiäänestyksestä syntyy tietovarantoja, niiden varmuuskopioita ja tietoliikenteen näytteitä, jotka ovat kokonaan tai osittain salattuja äänestyshetkellä. Käytettävissä olevan laskentatehon lisääntyminen (mukaan lukien kvanttilaskennan kehittäminen) ja salakirjoitusten avaamiseen (kryptoanalyysiin) liittyvät matemaattiset edistysaskeleet tarkoittavat, että nyt useimmilla menetelmillä salakirjoitetut tiedot ovat avattavissa tulevaisuudessa. Salakirjoituksen luotettava elinkaari on perinteisesti ollut korkeintaan kymmeniä vuosia; tällä hetkellä voimassa olevat salaussuositukset on annettu tyypillisesti vuosiin 2030–2040 asti. Jos jollakin toimijalla on keinoja säilyttää salakirjoitettuja tietoja, jotka on hankittu tietoliikennettä tiedustelemalla tai itse nettiäänestysjärjestelmästä, voi olla mahdollista, että tämä toimija saa yhdistettyä äänet äänestäjiin vielä heidän elinaikanaan.

6.2 Tiedon elinkaari

Nettiäänestyssovellus lähettää uurnaan sähköisesti vaalilippua vastaavat tiedot. Nettiäänestyssovelluksen käsittelemää tietoa on myös identiteetti, äänioikeus ja lokitiedot aikaleimoineen. Valtiollisten ja kunnallisten vaalien ja kansanäänestysten asiakirjoille on määritelty säilytysajat.

Taulukko 3: Asiakirjojen säilytys

Asiakirja	Valtiolliset vaalit	Kunnalliset vaalit	Kansanäänestys
Hyväksytyt äänestysliput	Hävitetään kun seuraavat vaalit on toimitettu	Hävitetään kun seuraavat vaalit on toimitettu	5 vuotta
Mitättömät äänestysliput	Hävitetään kun seuraavat vaalit on toimitettu	Hävitetään kun seuraavat vaalit on toimitettu	5 vuotta
Kotiäänestyslomakkeet	Hävitetään kun seuraavat vaalit on toimitettu	Hävitetään kun seuraavat vaalit on toimitettu	5 vuotta

Nykyisten määräysten mukaan äänestysliput ja kotiäänestyslomakkeet hävitetään, kun seuraavat vastaavat vaalit on toimitettu. Jos tätä sovelletaan nettiäänestysjärjestelmän sisältämään äänestysdataan, ei tiedon suojaamiselle tule salausmenetelmien elinkaaren kannalta ylitsepääsemättömiä haasteita. Säilytettävien tietojen muuttumattomuus tulee varmistaa, jotta lokitiedot pystytään tarkistamaan mahdollisten epäselvyyksien ilmetessä. Määrätyn säilytysajan jälkeen data olisi tällöin tuhottava kokonaan lokitietoineen.

Erona paperisiin äänestyslippuihin kuitenkin on, että lokitiedot, joilla on mahdollista selvittää väärinkäytöksiä, saattavat paljastuessaan johtaa vaalisalaisuuden heikentymiseen tai valitusta järjestelmästä riippuen jopa salaisuuden täydelliseen murtumiseen. Tämän takia on pidettävä huoli siitä, ettei datasta tehdä minkäänlaisia kopioita suojatun ympäristön ulkopuolelle. Nykymääräysten mukainen säilytys seuraaviin vaaleihin asti soveltuu vain tiedolle, joka ei paljastuessaan merkittävästi heikennä vaalisalaisuutta. Esimerkiksi Viron järjestelmässä allekirjoitetut äänet ja avaimet, joilla niiden salaus voidaan purkaa, hävitetään pian vaalien jälkeen.

Nettiäänten säilyttämisestä ei olisi vastaavaa hyötyä kuin paperiäänten säilyttämisestä. Nettiäänestyksessä ei voida suorittaa erillistä äänten tarkastuslaskentaa, joka mahdollistaisi ääntenlaskennassa tapahtuneiden virheiden löytämisen tai korjaamisen. Nettiäänestysjärjestelmässä täytyy luottaa järjestelmän tuottamaan tietoon siitä, mitkä äänet on otettu mukaan laskentaan. Mikäli tarkastuslaskenta nettiäänestysjärjestelmässä suoritettaisiin, se perustuisi järjestelmän tuottamaan tietoon ja antaisi

saman lopputuloksen kuin varsinainen laskenta. Sen sijaan nettiäänten sisällön paljastumisen riski kasvaa sitä mukaa mitä kauemmin niitä säilytetään.

Jokainen vaali on vaalitietojärjestelmän kannalta uusi tietojärjestelmäprojekti. Vaalien välillä tapahtuu muutoksia yhteiskunnassa ja tietojärjestelmiin tehdään päivityksiä. Virheiden ja manipuloinnin mahdollisuuden välttämiseksi jokainen nettiäänestysprojekti tulisi aloittaa puhtaalta pöydältä ja näin myös aina uudella uurnalla. Vanhojen uurnien käsittelyssä ja säilytyksessä on huomioitava kvanttilaskennan kehityksen tuomat uhat nykyisille salausteknologioille.

6.3 Tietojen tärkeysluokat ja suojaustasot

Nettiäänestysjärjestelmässä tiedon eheys nousee kriittisimmäksi ominaisuudeksi. Toiseksi, järjestelmän saatavuuden täytyy olla huipussaan äänestyksen ollessa käynnissä. Luottamuksellisuus on taas suoraan kytköksissä perustuslaissa ja vaalilaissa taattuun vaalisalaisuuteen ja osin tietosuojaan.

Henkilötietojen käsittelyä ja henkilörekistereitä ohjaavat henkilötietolaki, julkisuuslaki ja useat eri henkilötietojen käsittelyä koskevat erityislait, jotka asettavat erityisvaatimuksia mm. arkaluonteisten tietojen käsittelylle ja tietojen suojaamiselle.

Tietoturvallisuusasetuksen (681/2010) 9 §:n salassa pidettävien asiakirjojen luokitukset:

Suojaustaso I, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa ***erityisen suurta vahinkoa*** salassapitosäännöksessä tarkoitetulle yleiselle edulle;

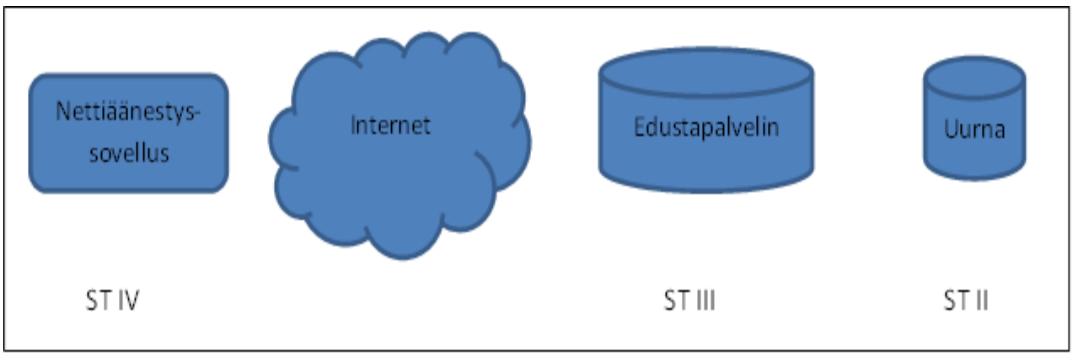
Suojaustaso II, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa ***merkittävää vahinkoa*** salassapitosäännöksessä tarkoitetulle yleiselle edulle;

Suojaustaso III, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa ***vahinkoa*** salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle;

Suojaustaso IV, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa ***haittaa*** salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle.

Henkilötiedot kuuluvat suojaustasolle III tai IV, mutta mikäli henkilötiedot sisältävät myös turvakiellon alaisten henkilöiden asuinpaikkoja, tulisi tieto luokitella suojaustasolle III. On myös huomioitava, että vaikka tietovarantoon sisältyvät yksittäiset asiakirjat olisivat julkisia tai alhaiseen suojaustasoon luokiteltavia, saattaa tietovaranto muodostaa kokonaisuuden, jonka suojaustarve on siihen sisältyviä yksittäisiä asiakirjoja korkeampi. Tällainen yhdistelmä syntyy, jos henkilötiedot ja henkilöiden äänet säilytetään yhdistettynä samassa järjestelmässä. Mikäli henkilötiedot pystyttäisiin erottamaan heti äänestystapahtuman jälkeen äänistä, tätä ongelmaa ei tulisi, mutta mahdollinen vaatimus siitä, että nettiääni pitää pystyä korvaamaan uudella nettiäänellä tai paperiäänellä edellyttää, että henkilötieto ja ääni pidetään yhdessä laskentaan asti.

Nettiäänestysjärjestelmän suuntaa-antavaan tärkeysluokitteluun on käytetty VAHTI:n suojattavien kohteiden (tietojärjestelmien) tärkeysluokittelutyökalua tukena. Työkalu ei suoraan sovellu tähän arviointiin, johtuen nettiäänestysjärjestelmän erityispiirteistä. Kriittisimmät vaatimukset kohdistuvat kahden viikon aikaikkunalle (ennakkoäänestysaika ja ääntenlaskenta). Ääniä säilytetään vain rajallinen aika, joten pitkäaikaissäilytystä ei varsinaisesti ole, jos uurna tämän jälkeen tuhotaan. Tietoturvallisuusasetuksen ja tärkeysluokittelun tuloksena nettiäänestysjärjestelmän osille on määritelty vaaditut suojaustasot.



Kuva 1: Suojaustasot nettiäänestysjärjestelmän osille

6.4 Tietosuoja

Keskeisin äänestystä koskeva tietosuojavaatimus on vaalisalaisuuden turvaaminen. Sen alkuperäinen tarkoitus on suojata äänestäjän vapautta antaa ääni haluamalleen ehdokkaalle vähentämällä mahdollisuutta painostustoimenpiteisiin. Samalla kaupankäynti äänillä hankaloituu. Vaalisalaisuutta itse äänestysjärjestelmän osalta käsitellään raportissa toisaalla.

Merkittävimmät nettiäänestysjärjestelmässä käsiteltävien henkilötietojen suojaan liittyvät seikat liittyvät sellaisiin käyttötapauksiin, joissa äänestäjän toimet voivat jättää esimerkiksi lokimerkintöjä palveluihin kirjautumisesta ja käytöstä tai joissa äänestäjää voidaan mahdollisesti seurata selaimen tai päätelaitteen kautta vaikkapa selainevästeiden tai muun nk. telemetriatiedon avulla. Näitä toimintoja ovat esimerkiksi

- äänestäjän tunnistaminen
- vaaliluettelojen (äänioikeutettujen listan) käsittely
- ehdokaslistojen selailu
- kryptografisen materiaalin (esimerkiksi avainten) toimittaminen äänestäjille, mikäli tarpeen äänestysprotokollan toteuttamiseksi
- päätelaitteiden ja sovelluskauppojen käytöstä kerättävä käyttötieto
- äänestysjärjestelmän auditointi- ja muusta lokituksesta kerättävät tiedot

Tietosuoja-aspektit voivat liittyä sekä vaalisalaisuuden heikentymiseen, että tavanomaisempiin tietosuojariskeihin. Tietosuojavaatimuksia seuraa lähinnä EU:n yleisestä tietosuoja-asetuksesta[18] (General Data Protection Regulation, GDPR) sekä sähköisen viestinnän tietosuojadirektiivin ja tulevan asetuksen toteuttavasta lainsäädännöstä.

Vaalisalaisuuden osalta todennäköisin uhkakuva on se, että annetussa äänessä mahdollisesti oleva aikaleima voidaan korreloida esimerkiksi päätelaitteen muun käytön, mainostusverkoston, muun verkkoselailun tai äänestystapahtuman lokitietojen kanssa. Äänestysjärjestelmän tulisi tästä syystä pitää annetun äänen aikaleima salassa yhtä hyvin kuin äänestäjän identiteetti. Annetusta äänestä ei tietenkään tulisi myöskään käydä ilmi, millä päätelaitteella tai mistä ääni on annettu.

Varsinaisen äänestystapahtuman ulkopuolella kertyvien henkilötietojen käyttöä on tarkasteltava kahdesta näkökulmasta. Henkilötietojen käsittely on sallittua lakisääteisen velvoitteen (tässä tapauksessa vaalien) järjestämiseksi, mutta vaalien järjestämiseen suoranaisesti liittymätön analyysi tulee pystyä perustelemaan jollakin muulla perusteella. Esimerkiksi nettiäänestysjärjestelmän lokitietojen analysointi voisi tuottaa mielenkiintoista tietoa kansalaisten informaatiotekniikan käytöstä. Analyysitarpeet ja eri tietolähteiden yhdistelyperiaatteet tulisi etukäteen kuvata, jotta tarvittavat käsittelyn perusteet voidaan varmistaa.

Poliittinen mielipide on tietosuoja-asetuksen tarkoittama erityinen henkilötietoryhmä. Tämän vuoksi erilaisten käyttäjäseuranta- ja analytiikkaratkaisujen hyödyntäminen äänestysjärjestelmään liittyvissä oheisjärjestelmissä tulee arvioida tarkasti. Järkevä

[18] EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679 annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)

perusvaatimus lienee, ettei nettiäänestysjärjestelmän mistään komponenteista, mukaan lukien äänestystapahtuman käynnistämiseen ja ehdokkaiden selailuun käytettävät sovellukset ja nettisivut, ole mitään integraatioita analytiikkajärjestelmiin tai -palveluihin. Jos sovelluksen kehittämiseen, väärinkäytösten havaitsemiseen tai muuhun käyttötilastointiin tarvitaan analytiikkaa, tarvittava data tulee tuottaa taustajärjestelmästä erikseen sitä varten toteutetulla ja riittävän anonymiteetin takaavalla mekanismilla.

Nettiäänestys toteutuessaan koskettaisi jokaista äänioikeutettua ja sen voidaan katsoa olevan korkeariskistä henkilötietojen käsittelyä[19]. Tämän vuoksi nettiäänestyksestä ja siihen liittyvistä oheisjärjestelmistä on toteutettava tietosuoja-asetuksen tarkoittama tietosuojaa koskeva vaikutustenarviointi (Data Protection Impact Assessment eli DPIA). Vaikutustenarvioinnin tulisi kattaa koko nettiäänestysjärjestelmä oheisjärjestelmineen, eikä rajoittua vain tekniseen äänestysprotokollaan.

Vaikutuksenarvioinnissa on tietosuoja-asetuksen mukaan arvioitava suunnitellut "suoja- ja turvallisuustoimet ja mekanismit". Vaikutustenarviointi tulisi tämän vuoksi teknisiltä osiltaan toteuttaa tietoturva-arvioinnin yhteydessä, jotta vaikutustenarvioinnissa on käytössä riittävän tarkka kuva sen teknisestä toteutuksesta ja suoja- ja turvallisuustoimien tasosta.

[19] GDPR vaatii tietosuojan vaikutustenarvioinnin mm. jos kyseessä on "laajamittainen käsittely, joka kohdistuu [...] erityisiin henkilötietoryhmiin". Järjestelmä käsittelee ääniä, jotka ilmaisevat poliittista mielipidettä, joten vaikutustenarviointi on jo tämän vuoksi pakollinen.

7 Äänestäminen internetissä

Nettiäänestäminen tulisi perinteisen paperiäänestyksen rinnalle, joten selkeyden ja ymmärrettävyyden vuoksi niissä tulisi pyrkiä noudattamaan mahdollisimman samankaltaista prosessia.

1. Henkilö tunnistautuu
2. Henkilö tekee äänestysvalinnan
3. Äänestyslippu lähetetään uurnaan
4. Henkilö saa vahvistuksen äänestyksen onnistumisesta
5. Vaalipäivänä äänet puretaan ja lasketaan
6. Äänestyksen tulos julkaistaan
7. Uurnassa varmistetaan, että äänten lukumäärä vastaa äänestäjien määrää

Nämä ovat prosessin päävaiheet. Toteutustavat ja mitä eri vaiheissa tapahtuu vaihtelevat ratkaisusta riippuen. Nettiäänestyksessä tulee pystyä varmistamaan vaalisalaisuus, varmennettavuus, vastuullisuus ja painostuksen estäminen.

7.1 Äänestämisen turvaaminen

Äänestäjän tunnistaminen

Äänestäjän tunnistuksessa voidaan käyttää vahvaa sähköistä tunnistautumista, allekirjoitusta, kertakäyttöistä koodia, tai näiden yhdistelmiä. Aiemmassa esiselvityksessä suositeltiin sähköistä henkilökorttia, koska kortti sisältää allekirjoittamisen mahdollistavan VRK:n varmenteen. Toisaalta pankkitunnistus, joka ei tue allekirjoitusta, on lähes kaikkien äänestäjien käytettävissä ja siten käytännöllisempi valinta.

Sähköisen tunnistamisen menetelmät vaikuttavat nettiäänestysjärjestelmän suunnitteluun. Esimerkiksi Viron järjestelmässä lähdetään siitä, että jokaisella äänestäjällä on allekirjoitusvarmenne. Mikäli halutaan käyttää pankkitunnistusta yhdessä sellaisen

nettiäänestysjärjestelmän kanssa, jossa äänestäjä allekirjoittaa antamansa äänen, joudutaan sähköinen allekirjoitus toteuttamaan ohjelmallisesti käyttäjän päätelaitteella. Lisäksi äänen allekirjoitusta varten pitää luoda ohjelmallisesti kertakäyttöinen avainpari. Tällainen allekirjoitus ei täyttäisi yllä mainittuja korotetun tai korkean varmuustason vaatimuksia, joten se pitäisi ymmärtää äänestysjärjestelmän sisäiseksi toiminnoksi eikä eIDAS-asetuksen mukaiseksi sähköiseksi allekirjoitukseksi. Tietoturvan kannalta erityisen ongelmallista olisi sähköisen allekirjoituksen toteuttaminen äänestäjän nettiselaimessa. Toisaalta, jos äänestysmenetelmä valitaan niin, että se vaatii vain käyttäjän sähköisen tunnistamisen eikä allekirjoitusta, menetetään mahdollisuus jo annettujen äänten aitouden auditointiin allekirjoitusten perusteella. Tällöin äänen lähettämisestä ja vastaanotosta tulee erityisen herkkä kohta järjestelmän turvallisuuden kannalta.

Vaalisalaisuus

Vaalisalaisuus nettiäänestysjärjestelmissä turvataan kryptografisella salauksella. Salauksen tulee tapahtua jo äänestyssovelluksessa ja purun vasta suojatussa uurnassa. Yksi menetelmä salaukseen on julkisen avaimen salaus ja varmenteet. Tällöin äänet salataan äänestyssovelluksessa vaalijärjestelmän julkisella avaimella, ja salaus puretaan ääntenlaskentaa varten järjestelmän yksityisellä avaimella. Toinen tapa on lähettää esimerkiksi postitse äänestäjälle henkilökohtainen tunniste, jolla ääni salataan. (Tässä on huomattava, ettei pelkästään postitse lähetettävän koodin avulla pysty äänestämään, vaan tämän lisäksi tulee varmistua, että äänestäjä on tunnistettu ja hänellä on äänioikeus.) Ennen äänten avaamista ja laskentaa salatut äänet pitää sekoittaa uurnassa niin, ettei laskettuja ääniä ole mahdollista yhdistää annettuihin. Sekoitus pitää kuitenkin tehdä niin, ettei ääniä myöskään ole mahdollista lisätä, poistaa tai vaihtaa. Elektronisten äänten sekoitukseen ja laskentaan on erilaisia kryptografiaan ja luottamuksen hajauttamiseen perustuvia menetelmiä (homomorfinen salaus, mix). Yksi tekninen ratkaisu ei ole sinänsä parempi kuin muut, vaan valinta riippuu järjestelmän kokonaisuudesta. Lopullinen ratkaisu käytettävästä menetelmästä tulee tehdä jonkin olemassa olevan järjestelmän pohjalta sitä tarpeen mukaan muokaten, kun ensin on selvillä nettiäänestyksessä noudatettavat reunaehdot.

Varmennettavuus

Äänestysketjun päästä päähän varmennettavuudella (end-to-end verifiability, E2E-V) tarkoitetaan sähköisen äänestysjärjestelmän ominaisuuksia, joiden avulla voidaan varmistua äänestystuloksen eheydestä. Varmennettavuutta on lähestytty kahdella eri tavalla. Kirjallisuudessa yleisempi tapa on jakaa tämä yksilölliseen ja universaaliin varmennettavuuteen (individual/universal verifiability).

1. Äänestäjä voi varmistaa, että hänen äänensä laskettiin sen ehdokkaan hyväksi, jota hän päätelaitteellaan äänesti. (individual verifiability)
2. Kuka tahansa voi varmistua siitä, että kaikki äänet on laskettu oikein. (universal verifiability)

Samoista vaatimuksista on olemassa myös vastaava versio:

1. Cast-as-intended: Ääni annetaan sellaisena kuin on tarkoitus
2. Recorded-as-cast: Ääni tallennetaan, kuten on annettu
3. Counted-as-recorded: Ääni lasketaan, kuten on tallennettu

Molemmissa vaatimusten esitystavoissa on tavoitteena varmistaa äänestysketjun eheys, ja lähestymistavat poikkeavat toisistaan lähinnä varmistuspisteiden osalta. Yksilölliseen/universaaliin varmennettavuuteen liittyen on esitetty[20] kritiikkiä, että tämä lähestymistapa ei takaisi päästä päähän varmennettavuutta, koska se tuottaa kaksi toisistaan erillistä tilannekuvaa eikä tosiasiassa takaa koko ketjua päästä päähän. Nettiäänestysjärjestelmien suunnittelussa kuitenkin käytetään tätä vaatimusmäärittelyä yleisesti, joten sitä käytetään myös tässä yhteydessä.

Ensimmäinen vaatimus tarkoittaa käytännössä sitä, että äänestäjällä on käytössään toiminto, jolla hän voi varmistaa, että oma ääni on laskettu oikealle ehdokkaalle. Vahvimmillaan varmennettavuus on, jos äänestäjä voi tehdä sen itsenäisesti saamiensa todisteiden perusteella, luottamatta lainkaan äänestysjärjestelmään. Jos tarkistamiseen käytettävä toiminto on osa itse äänestysjärjestelmää tai vaatii luottamusta sen johonkin osaan, voi varmennettavuuden ajatella toteutuvan vain osittain. Äänestäjän on tällöin edelleen luotettava siihen, että äänestysjärjestelmä raportoi äänen kirjautumisesta oikein.

Koska äänestäjän oman laitteen tietoturvasta ei ole mahdollista varmistua tietoteknisin menetelmin, voidaan sitä pitää erityisen haavoittuvana osana äänestysketjussa. Esimerkiksi haittaohjelma voisi vaihtaa äänen toiseksi tai hukata sen. Tällaiset väärinkäytökset voidaan havaita, jos äänestäjän on mahdollista tarkistaa riippumatonta paluukanavaa pitkin, että keskitetty järjestelmä on vastaanottanut hänen äänensä oikein. Äänen tarkistaminen tarkoittaa käytännössä datan siirtämistä ulos suojatusta ympäristöstä luokittelemattomaan paluukanavaan (esimerkiksi sähköposti tai mobiiliverkko). Suoraviivaisin ratkaisu on sisällön ilmaiseva: Tarkistuskuittauksen vastauksena on ”Kyllä, ääni on otettu annetun ja aiotun mukaisena huomioon ja laskentaan”. Varsinainen haaste piilee siinä, ettei itse äänen sisältöä voida palauttaa paluuviestissä, koska todiste annetusta äänestä mahdollistaisi äänten myymisen. Luottamuksen lisäämisen

[20] Cryptographic Security Analysis of E-voting Systems: Achievements, Misconceptions, and Limitations, Küsters, Müller, Electronic Voting, 2017.

kannalta on kuitenkin haitallista, että äänestäjälle ei kerrota kokonaistietoa. Virossa tämä on ratkaistu siten, että äänestäjä saa rajatun ajan QR-koodin kautta tarkistaa äänen sisällön. Äänten ostamista on vaikeutettu lisäksi uudelleenäänestämisellä: äänensä myynyt voi myöhemmin vaihtaa äänen toiseksi.

Toinen vaatimus tarkoittaa, että kuka tahansa äänestäjä tai ulkopuolinen auditoija voi tarkistaa, että kaikki äänet on laskettu oikein. Tämä toteutuu osittain Suomen vaalikäytännössä, jossa äänestäneiden luettelo on julkinen. Tämä mahdollistaa sen arvioinnin, vastaako vahvistettu tulos äänestäneiden lukumäärää. Paperiäänestyksessä myös itse äänestysliput on mahdollista tarkistaa. Vaalisalaisuutta vaativassa sähköisessä äänestyksessä universaali varmennettavuus toteutetaan yleensä julkistamalla annetuista äänistä taulukko, josta kukin äänioikeutettu voi tarkistaa henkilökohtaisen koodin avulla joko, että hänen äänensä on laskettu oikein, tai mikäli hän ei ole äänestänyt, ettei ääntä ole taulukossa. Väärinkäytökset havaitaan todennäköisesti, kun riittävä osa äänioikeutetuista tarkistaa omat tietonsa. Norjassa käytettiin tätä ratkaisua ja äänet julkaistiin sanomalehdessä.

Toinen vaatimus voidaan myös toteuttaa äänestysketjussa vaihe vaiheelta siten, että riippumattomat auditoijat varmistuvat kunkin ketjun vaiheen eheydestä kahdennettujen toimintojen tai kryptografisten todistusten kautta. Tällaiseen auditointiin osallistuvien tahojen pitäisi olla täysin itsenäisiä tarvittavia ohjelmistoja myöten. Tämä vaatimus useista itsenäisistä auditoijista valitettavasti lisää sekä nettiäänestysjärjestelmän kustannuksia, että ohjelmistojen virheiden ja yhteensopivuusongelmien vuoksi syntyvien virheellisten hälytysten mahdollisuutta.

Tärkeää on huomata, että äänestysketjun varmennettavuus on osittain ristiriitainen vaatimus vaalisalaisuuden kanssa. Tämä johtuu siitä, että järjestelmässä joudutaan varmennettavuutta varten säilyttämään äänestäjät ja äänet toisiinsa yhdistävää tietoa. Erityisesti jos halutaan, että varmettavuuden ansiosta havaitut väärinkäytökset on mahdollista myös tutkia ja todistaa, on järjestelmään rakennettava takaportti vaalisalaisuuden osittaiseksi purkamiseksi. Yksittäisen äänestäjän käsissä tällainen takaportti voisi johtaa äänten myymiseen, ja vaaliviranomaisten käsissä se voisi pahimmillaan johtaa vaalisalaisuuden laajamittaiseen murtumiseen. Nettiäänestysjärjestelmän vaatimuksia määritellessä joudutaan siis tekemään valintoja vahvan vaalisalaisuuden ja vahvan varmennettavuuden välillä. Suomessa vaalisalaisuutta on yleensä pidetty ehdottomana vaatimuksena, joten käytännössä nettiäänestysjärjestelmä ei voi tukea täydellistä päästä-päähän varmennettavuutta.

Vaalisalaisuuden takia on siis mahdollista, että äänestäjä tai järjestelmä havaitsee väärinkäytöksen, muttei pysty selvittämään tai korjaamaan sitä. Tämän vuoksi onkin keskeistä määritellä ennalta toimintatavat, kun äänestäjä tai muun osapuoli ilmoittaa havainneensa virheen äänestysketjussa. Toimintatavat pitää määritellä myös tilantei-

siin, joissa kukaan muu kuin väitteen esittäjä ei pysty tarkistamaan sen todenperäisyyttä. Tällaisten tilanteiden asianmukainen käsittely on keskeistä vaalituloksen legitimiteetin ja sähköisen äänestämisen yleisen luottamuksen kannalta.

Äänestysjärjestelmän tekniselle toteutukselle äänestysketjun päästä päähän varmennettavuus on siis hyvin haastava vaatimus. Markkinoilla on toteutuksia, joissa edellä mainitut vaatimukset toteutuvat eri tavoilla. Vaalisalaisuuden turvaamiseksi joudutaan kuitenkin aina hyväksymään jonkin verran epävarmuutta, ja sen käsittelyyn on varauduttava menettelytavoilla ja lainsäädännöllä.

Vastuullisuus

Vastuullisuus (accountability) on varmennettavuuden kehittyneempi aste. Ei riitä, että varmistetaan äänen virheetön toimitus laskentaan, vaan tulee myös tunnistaa mahdollinen manipulointi tai ääniin vaikuttava tekijä, sulkea se pois järjestelmästä sekä tuottaa mahdolliseen rikossyytteeseen riittävät todisteet. Käytännössä tämä tarkoittaa, että vaaleista vastaavan organisaation tulee pystyä varmistamaan äänten ja lopputuloksen oikeellisuus jopa paremmin kuin paperijärjestelmässä. Aihetta on vielä tutkittu varsin vähän, mutta sen merkitys on tiedostettu.

Vastuullisuuden riippuvuus järjestelmän teknisestä toimittajasta on noussut tässä yhteydessä esille, ja esimerkiksi Itävallassa[21] on päädytty siihen, että vaaliorganisaation tulee pystyä täyttämään vastuullisuusvaatimukset itsenäisesti, ulkopuolisesta asiantuntijasta riippumattomasti.

Painostuksen estäminen

Äänestyksen siirtyessä valvomattomiin olosuhteisiin tulee painostuksen (coercion) ja äänten myymisen mahdollisuus eri tavalla esiin kuin valvotussa äänestämisessä äänestyspaikalla. Kotona tai muussa valvomattomassa paikassa äänestäjä on itse vastuussa valinnanvapauden ja vaalisalaisuuden säilymisestä, eikä vaaliviranomainen pysty havaitsemaan poikkeamia. Jo pelko siitä, että esimerkiksi perheenjäsenet näkevät äänen, saattaa heikentää äänestäjän todellista vapautta valita haluamansa ehdokas.

Keskeisin keino painostuksen ja äänten myynnin estämiseen on, se ettei nettiäänestysjärjestelmästä pysty saamaan mitään todistetta tai kuittia siitä, mitä on äänestänyt.

[21] Voting in E-Participation: A Set of Requirements to Support Accountability and Trust by Electoral Committees. Peter Parycek1, Michael Sachs, Shefali Virkar and Robert Krimmer. Electronic Voting. 2017.

Kuten edellä on selitetty, tässä tulee esiin ristiriita varmennettavuuden kanssa. Varmennettavuus edellyttää, että käyttäjä voi todentaa, että ääni on mennyt oikein perille. Nettiäänestysjärjestelmissä on hyvin erilaisia ratkaisuja tähän varmentamiseen, mutta mikään ratkaisuista ei ole selkeästi noussut ylitse muiden. Äänten ostamista on vaikeutettu lisäksi uudelleenäänestämisellä: äänensä myynyt tai painostuksen kohteeksi joutunut voi myöhemmin vaihtaa äänen toiseksi ja lopulta korvata sähköisen äänen paperiäänellä. Tätä on pidetty joissain ratkaisuissa toimivana keinona ehkäistä äänten myyntiä, mutta on epäselvää, kuinka hyvin keinot todellisuudessa suojaavat henkilöitä, jotka joutuvat arkielämässään tarkkailun tai painostuksen kohteeksi.

Päästä päähän todennettavuuden keinona toimivaan julkiseen tulostaulukkoon liittyy riski, että painostaja huomaa taulukon julkaisun jälkeen, että ääntä on muutettu. Protokollien kehityksessä on tullut esille erityyppisiä ratkaisuja, joissa sovellus tuottaa oikeiden äänten lisäksi ns. valeääniä, mutta täysin ei painostusta näillä ratkaisuilla voi sulkea pois.

7.2 Lohkoketjuilla eheyttä?

Lohkoketju on viime aikoina esiin noussut menetelmä, jota on esitetty mahdollisena ratkaisuna vastuullisuuden lisäämiseen nettiäänestysjärjestelmässä. Muun muassa Euroopan Parlamentin tutkimuspalvelu on vastikään selvittänyt lohkoketjujen käyttöä nettiäänestyksessä[22].

Lohkoketju (*blockchain*) on digitaalinen reskontra tai tapahtumalista[23], jonka kirjaukset on tallennettu lohkoiksi kutsuttuihin tietorakenteisiin, jotka on ketjutettu toisiinsa kryptografisesti. Ketjun kirjausten eheydestä voidaan varmistua tarkastamalla ketjun kryptografiset linkit. Lohkoketjut on tehnyt erityisesti tunnetuksi kryptovaluutta Bitcoin, jonka transaktiot kirjataan lohkoketjuun. Tekniikkana lohkoketju soveltuu omaan käyttökohteeseensa eli auditoitavan ja hankalasti väärennettävän tapahtumalistan tai lokin ylläpitoon. Esimerkiksi järjestelmät voivat lisätä tapahtumien auditoinnin uskottavuutta käyttämällä lohkoketjuja tai muita vastaavia julkisia tapahtumalokeja.

---

[22] Esimerkiksi Marko Kovic: *Blockchain for the people*, 2017 (https://osf.io/preprints/socarxiv/9qdz3) sekä Euroopan parlamentin tutkimuspalvelun lyhyt julkaisu *What if blockchain technology revolutionised voting?*, 2016 (http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA%282016%29581918_EN.pdf).

[23] Liikenne- ja viestintäministeriön raportissa *Lohkoketjuteknologian soveltaminen ja vaikutukset liikenteessä ja viestinnässä* on hyvä suomenkielinen selitys lohkoketjun tekniikasta. http://julkaisut.valtioneuvosto.fi/handle/10024/80667

Kun keskustellaan lohkoketjujen käytöstä nettiäänestyksessä, olisi kuitenkin aina pyrittävä esittämään tiettyä ja nimenomaista lohkoketjun käyttökohdetta mieluiten nimetyn nettiäänestysjärjestelmän viitekehyksessä. Jos lohkoketjun käyttökohde edellyttää sen hajauttamista, tekniikan käytön ehdotuksessa tulisi myös ottaa kantaa hajautetun toteutuksen osallistujiin, lohkoketjun konsensusalgoritmiin sekä lohkoketjuun tallennettujen tietojen luottamuksellisuuteen ennen kuin ehdotuksesta voidaan rakentavasti keskustella.

Lohkoketjujen erityinen ominaisuus on, että ne voivat olla hajautettuja. Lohkoketjuun perustuvaa reskontraa varten ei tällöin tarvitse olla yhtä, luotettua tahoa, vaan useat eri tahot voivat ehdottaa uusia lohkoja lisättäväksi lohkoketjuun. Tämä saattaisi johtaa lohkoketjun haarautumiseen, mutta loppujen lopuksi voi olla kuitenkin vain yksi, paikkansa pitävä lohkoketju. Tämän vuoksi lohkoketjuun lisättävät lohkot päätetään jollakin konsensusalgoritmilla (*consensus algorithm*). Konsensusalgoritmi huolehtii siitä, että yksittäinen taho ei voi yksin sanella lohkoketjun sisältöä. Esimerkiksi uutiskynnyksenkin useasti ylittänyt Bitcoinin "louhinta" liittyy sen konsensusalgoritmin toteutukseen.

Hajautetussa lohkoketjussa tarvittavan konsensusalgoritmin valinta ei nettiäänestyksessä ole suoraviivaista. Konsensusalgoritmissa tulee huomioida teknisen toteutuksen lisäksi algoritmin osallistujat ja insentiivimalli. Monissa ehdotetuissa lohkoketjuissa osallistujat pyritään hajauttamaan mahdollisimman laajalti eri maihin. Tämä hajauttaminen tarkoittaa, että lohkoketjun käyttö on riippuvainen kansainvälisistä internetyhteyksistä, mikä voi aiheuttaa ongelmia vaalijärjestelmän saavutettavuudelle äänestyksen aikana. Kryptovaluutoissa insentiivimalli perustuu useimmiten joko rahan ansaitsemiseen tai olemassa olevan sijoitetun pääoman säilyttämiseen. Vaaleissa konsensusprotokollan ja insentiivimallin tulisi taata kilpailevien puolueiden ja yksittäisten äänestäjien yhdenvertaisuus. Konsensusalgoritmi ei saisi myöskään tuoda lisää mahdollisuuksia asettaa vaalitulosta kyseenalaiseksi, esimerkiksi niin, että jokin taho toisi julki vaihtoehtoisia konsensuksia, jotka söisivät uskoa siihen, mikä on kulloinkin oikea lohkoketjun haara. Jos lohkoketju on yhden tahon, esimerkiksi vaaliviranomaisen, hallinnassa, kysymys konsensusalgoritmista ei ole niin olennainen, mutta samalla osa lohkoketjun lupauksista mahdollisesti menetetään.

Mikäli lohkoketju on hajautettu, lohkoketju on nähtävä käytännössä "ikuisena" tietorakenteena, koska siitä muodostuu kopioita, joita ei myöhemmin todennäköisesti voida lopullisesti tuhota. Tämän vuoksi hajautetusti ylläpidettyyn lohkoketjuun tallennettavien tietojen tulee olla joko julkisia, tai mikäli tiedot ovat salattuja, tulevaisuudessa tapahtuva salauksen murtaminen ei saisi aiheuttaa ongelmia. Tällä hetkellä kryptografisista algoritmeista annetaan suosituksia tyypillisesti 15–25 vuoden päähän tulevaisuuteen, eikä kvanttilaskennan tuoma kryptografisen laskennan tehostuminen ole vielä lopullisesti ymmärretty aihealue. Mikäli lohkoketju sisältäisi salattuja ääniä, joiden

avulla vaalisalaisuus voisi murtua, tämä riski olisi otettava huomioon. Mikäli hajautettu lohkoketju sisältäisi suoranaisesti henkilötietoja, näiden käsittelyn tarkoituksen on pysyttävä laillisena niin ikään rajattomasti, sillä lohkoketjusta ei teknisesti voida poistaa tietoa poistopyynnön seurauksena. Huomioitava on, että nykyisetkään vaalien arkistointikäytännöt eivät edellytä äänien säilyttämistä seuraavien vaalien jälkeen, joten ”ikuinen” lohkoketju ei tästä näkökulmasta ole tarpeen.

Salausavaimien hallinnointiin liittyy myös tiettyjä haasteita. Mikäli kaikissa vaaleissa käytetään samaa lohkoketjua niin salausalgoritmin vaihtaminen vaaleista toiseen voi olla haasteellista. Jos jokaisella vaalilla on oma lohkoketjunsa, niiden hallinnointi menisi monimutkaiseksi.

8 Tietoturvallisuusvaatimukset

Äänestyksessä tietoturvan kannalta merkittävimmät vaatimukset kohdistuvat vaalisalaisuuden ja äänestystuloksen oikeellisuuden varmistamiseen. Tietoturvallisuus tulee huomioida kehitystyön, käyttöönoton ja ylläpidon kaikissa vaiheissa. Tietoturvaa ei ole mahdollista varmistaa vain käyttöönoton kynnyksellä tehtävällä laajalla tietoturva-auditoinnilla, vaan tietoturvan tulee olla luonnollinen osa tekemistä.

Tietoturvatekijöiden määritelmät

Saatavuus

Äänestysjärjestelmän tulee olla äänestäjien käytettävissä koko vaalin äänestysvaiheen ajan. Äänestystulos tulee olla saatavilla ja tiedon siirrettävissä äänestyksen päätyttyä.

Luottamuksellisuus

Vaalisalaisuus tulee kyetä suojaamaan paljastumiselta äänestyksen aikana ja sen jälkeen. Annettua ääntä ei saa pystyä kiistatta kytkemään äänestäjään.

Eheys

Äänestystuloksen tulee perustua äänestäjien ilmaisemaan tahtoon. Ääniä ei saa syntyä tyhjästä, mutta niitä ei saa myöskään hävitä.

Kiistämättömyys

Äänestysprosessin tulee olla läpinäkyvä ja valvonnan kyetä varmistamaan, että äänestystulokseen voidaan luottaa. Valvonnan tulee myös kyetä tietoon perustuen tukemaan omaa näkemystään esitettyjä epäilyjä vastaan.

Tunnistus

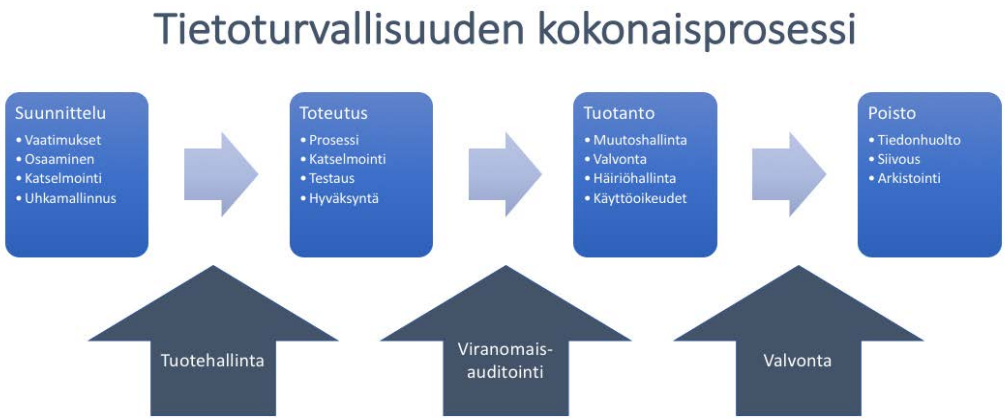
Kaikkien järjestelmän käyttäjien (äänestäjä, pääkäyttäjä, valvoja yms.) tulee olla tunnistettuja ja identiteetti varmistettu.

Todennus

Äänestäjällä tulee olla vain oikeus antaa ääni omissa nimissään, eikä tällä saa olla pääsyä muiden äänestäjiä koskevaan tietoon. Järjestelmän käyttäjillä tulee olla vain rooliinsa kuuluvat oikeudet järjestelmän tietoihin.

8.1 Tietoturvallisuuden varmistaminen

Tietoturva tulee huomioida palvelun koko elinkaaren ajan osana laadunvarmistusta. Sen tulee kattaa palvelun suunnittelu, toteutus, käyttöönotto, sekä järjestelmän käytöstä poisto. Vasta tuotantovalmiuden saavutettua suoritetaan viranomaisauditointi, jolla varmistetaan päätettyjen tietoturvavaatimuksien täyttyminen. Viranomaisauditointi toimii porttina tuotantokäytölle ja lähtökohtaisesti tietoturva on otettu huomioon kaikissa sitä edeltävissä vaiheissa.



Kuva 4: Tietoturvallisuuden kokonaisprosessi

Esiselvityksessä tunnistetut riskit ja tietoturvavaatimukset tulee huomioida projektisoinnissa ja suunnitteluvaiheessa. Tällöin tulee kiinnittää huomioita myös toteutuksessa tarvittavaan erityisosaamiseen ja varmistaa, että resursointi vastaa tätä tarvetta. Ratkaisusuunnitelman osalta tulee suorittaa uhkamallinnus, sekä toteutuksen lopputuotoksien testauskäytännöt tulee olla määritelty ennen toteutuksen alkua.

8.2 Turvallinen ohjelmistokehitys

Ohjelmistokehitys on prosessi, jossa tavoitteenmukainen ohjelmisto toteutetaan, otetaan käyttöön, ylläpidetään ja lopulta poistetaan käytöstä hallitusti. *Turvallinen* ohjelmistokehitys (*security* tai *secure software development lifecycle, SDLC* tai *S-SDLC*) pyrkii siihen, että käytössä oleva ohjelmisto ei ainoastaan täytä sille asetettuja toiminnallisia tavoitteita, vaan myös sen elinkaaren eri vaiheissa kohtaamat turvallisuustarpeet.

Ohjelmiston turvallisuustarpeita on usein hyvin hankala määritellä täsmällisesti ja kokonaisvaltaisesti. Tämä johtuu siitä, että suuri osa turvallisuudesta liittyy järjestelmän järkevään ja ennustettavaan toimintaan myös sellaisissa tilanteissa, joita ei kehityksen aikana osattu ennakoida. Toiminnalliset tietoturvavaatimukset eivät välttämättä takaa lopputuotteen tietoturvallisuutta. Tunnettu mediakynnyksen ylittänyt esimerkki on taannoinen Heartbleediksi[24] nimetty haavoittuvuus, jossa salausprotokollan toteutusvirhe mahdollisti salausavainten varastamisen.

Ohjelmistoturvallisuuden mittaaminen on haastavaa, koska esimerkiksi tietoturvatestaus voi ainoastaan paljastaa tietoturvapuutteiden olemassaolon. Täyttä varmuutta tietoturvasta ei voida testauksella saavuttaa, sillä osa puutteista voi jäädä havaitsematta ja päätyä tuotantoon. Testaus onkin vain yksi niistä aktiviteeteista, joiden kautta järjestelmä voidaan jollakin luotettavuustasolla olettaa tietoturvalliseksi.

Edellä kuvatusta johtuen turvallista ohjelmistokehitystä kuvaavat mallit ovat varsin monitahoisia. Tunnetuin ja ajantasaisin, noin sadan organisaation kvalitatiiviseen haastattelututkimukseen perustuva malli BSIMM[25] (*Building Security In Maturity Model*) jakaa ohjelmistoturvallisuuden 12 osa-alueeseen ja näiden sisällä 113 eri aktiviteettiin. Ohjelmistokehitysorganisaatiot suorittavat näistä aktiviteeteista yleensä vain jonkin osajoukon, jolle on liiketoiminnan osalta selkeä tilaus. Aktiviteetteja ei voida laittaa absoluuttiseen tärkeysjärjestykseen, vaan niiden tärkeys voi vaihdella organisaation kulttuurin, rakenteen, taitotason, rahoituksen, viranomais- ja muiden vaati-

[24] http://heartbleed.com/
[25] https://www.bsimm.com/framework.html

musten sekä tuotettavan ohjelmiston mukaan. Suomen valtionhallinnon näkökulmasta aktiviteettien priorisointia on kuvattu VAHTI-ohjeessa 1/2013[26].

Nimenomaan ohjelmiston teknisen toteutuksen aikana tärkeimpinä aktiviteetteina voidaan pitää asiantuntevaa vaatimusten määrittelyä ja tuoteomistajuutta, arkkitehtuurin puolustuksellista suunnittelua ja riskianalyysiä (uhkamallinnusta), suunnittelu- ja koodikatselmointeja, tutkivaa tietoturvatestausta, haavoittuvuuksien seurantaa ja hallintaa sekä käytönaikaista seurantaa. Kriittisen järjestelmän ohjelmistokehitysprosessin pitäisi pystyä tuottamaan näyttöä siitä, että ainakin kaikkia näitä aktiviteetteja on suoritettu.

Turvallisen ohjelmistokehityksen aktiviteetteja tulisi toteuttaa mahdollisimman aikaisessa vaiheessa kustannustehokkuuden vuoksi ja vaikutuksen maksimoimiseksi. Perinteisesti tämä tarkoittaa vaatimusmäärittely- ja suunnitteluvaihetta, tyypillisesti arkkitehtuurin ja toteutusperiaatteiden katselmointeja. Nykyaikaisessa ohjelmistokehityksessä (ketterässä kehityksessä) nämä vaiheet toistuvat iteratiivisesti ja yhä uudelleen, joten ohjelmistoturvallisuusaktiviteetitkin tulee tällöin siirtää osaksi jatkuvaa toteutusprosessia.

Tietoturvan "lisääminen" järjestelmään jälkikäteisesti esimerkiksi testaamalla on ainoana aktiviteettina joko tehotonta tai riittämätöntä. Ostettaessa valmiita ohjelmistotuotteita tai osakomponentteja, toimittajalta on vaadittava erikseen näyttö siitä, että turvallisia ohjelmistokehityksen aktiviteetteja on tehty koko ohjelmistokehityksen ajan.

Nettiäänestysjärjestelmän riskien johdosta on perusteltua edellyttää toimittajilta näyttöä ohjelmistoturvallisuusaktiviteettien kattavasta noudattamisesta tuotteensa määrittelyssä, suunnittelussa ja toteutuksessa. Samoin itse toteutus- ja integraatioprojektissa alueen aktiviteetteihin on varmistettava riittävät resurssit ja osaaminen.

Kehitys

Kaikilla toteutukseen osallistuvilla henkilöillä tulee olla perustietämys tietoturvasta omaan osaamisalueeseensa liittyen ja kehityksessä tulee noudattaa VAHTI 1/2013 Sovelluskehityksen tietoturvaohjetta. Erityistä huomiota tulee käyttää ratkaisuissa käytettyihin salausratkaisuihin ja avainhallintaan, jonka tulee noudattaa VAHTI 2/2015 Ohje salauskäytännöistä -ohjetta.[27]

[26] VAHTI 1/2013 Sovelluskehityksen tietoturvaohje, https://www.vahtiohje.fi/web/guest/vahti-1/2013-sovelluskehityksen-tietoturvaohje
[27] https://www.vahtiohje.fi/web/guest/2/2015-ohje-salauskaytannoista

Kullekin ratkaisusuunnitelmien kokonaisuudelle tulee toteuttaa määrämuotoinen uhkamallinnus, jolla tunnistetaan ratkaisua koskevien toiminnallisten tietoturvavaatimuksien eheys.

Kehityksen tuotoksien osalta tulee aina varmistua toteutuksen tietoturvan efektiivisyydestä ja tietoturvan varmistaminen tulee sisältyä kaikkiin testausvaiheisiin oleellisena osana.

Kehitysvaiheessa tulee laatia ja testata palvelukomponenttien toipumissuunnitelmat, palvelun jatkuvuussuunnitelma, sekä varautumissuunnitelma. Näiden osalta tulee noudattaa VAHTI 2/2016 Toiminnan jatkuvuuden hallinta-ohjetta. [28]

Käyttöönotto

Osana käyttöönottovaihetta toteutetaan kattava harjoittelu, jolla varmistetaan palvelukokonaisuuden tuotantokelpoisuus. Harjoitukseen tulee sisältyä:

- Normaali toiminta
- Häiriöselvitys
- Jatkuvuuden hallinta
- Varautumissuunnitelmat

Ylläpito ja käytöstä poisto

Palvelutuotannon tulee noudattaa hyvää tietohallintotapaa ja sen tulee kyetä havaitsemaan tekijät, joita tulee analysoida tarkemmin uhkien havaitsemiseksi. Analyysin perustella käynnistetään kehitystyötä tai rajoitetaan palvelun toiminnallisuuksia.

Vaalien äänestyksen aikana järjestelmään ei tulisi kohdistua ylläpidollisia toimia, jotka voivat vaarantaa äänestystuloksen. Järjestelmän tulisi toimia automaattina, jonka tilaa kyetään valvomaan ja mahdollisen häiriön jälkeinen palautuminen normaaliin tapahtuu vaalitulosta vaarantamatta.

Vaalien päätyttyä operatiivinen tieto tulee hallitusti poistaa tai arkistoida ilman, että tiedon suojaus heikkenee. Arkistoitu tieto tulee suojata tiedon muuttumiselta ja analyysimenetelmin suoritetusta äänestystiedon johtamiselta sekä tuhota turvallisesti säilytysajan päätyttyä.

[28] https://www.vahtiohje.fi/web/guest/vahti-2/2016

Auditointi

Toteutusvaiheen aikana varmistetaan kunkin lopputuotteen osalta laadukkuus kattavalla testauksella, johon kuuluu osana tietoturvatestaus. Tuotantovalmius eri osa-alueille todennetaan testaustulosten perusteella, jonka jälkeen järjestelmä jää odottamaan viranomaisauditoinnin valmistumista.

Palvelun infrastruktuurin saavutettua tuotantovalmiuden, voidaan aloittaa palvelutuotannon viranomaisauditointi, joka tehdään kullekin palveluosalle päätetyn suojaustason mukaisesti. Tässä voidaan käyttää Viestintäviraston hyväksymää tietoturvallisuuden arviointilaitosta ST-IV ja ST-III suojaustasoilla, jonka lisäksi Viestintäviraston tulee täydentää ST-II suojaustason osalta arviointilaitoksen tekemä ST-III tarkastus. Viestintäviraston hyväksyntä palvelulle on edellytys ehdoton edellytys tuotannon aloittamiselle (hyväksyntä perustuu auditointiraporttiin).

Viranomaisauditoinnin tulee kattaa kokonaisuudessaan (KATAKRI 2015 ST-IV/ST-III/ST-II)

- Palvelutuotannon ohjaus ja muutoshallinta (palvelinhallinta, tietoliikenneverkot ja sovellukset)
- Julkaisunhallinta (sovellukset)
- Tukipalvelut (esim. Service Desk)
- Käyttöpalvelut ja palvelutuotanto (palvelimet ja tietoliikenneverkot)
- Käyttöympäristöjen fyysinen turvallisuus
- Palveluun liittyvät osapuolet (esim. Suomi.fi- palvelut)
- Salausratkaisuiden arviointi
- Palvelun käyttöliittymät ja web-palveluportaali
- Jatkuvuussuunnitelmat ja varautuminen

Kunkin vaalin alussa ja lopussa tulee varmistaa tarkastuslistoin, että järjestelmän tila vastaa vaihetta ja järjestelmässä ei ole väärää tai poistettavaa tietoa.

9 Tavoiteratkaisun kuvaus

9.1 Järjestelmän toiminnallisuus

Yleiset vaalit

Nettiäänestystä varten äänioikeutettu tarvitsee vahvat sähköisen tunnistuksen välineet, päätelaitteen ja internet-yhteyden. Tässä esiselvityksessä ei oteta kantaa siihen, onko päätelaite tietokone, mobiililaite tai muu internetyhteydellä varustettu laite.

Käyttäjä tunnistautuu vahvaa sähköistä tunnistusta käyttäen ja tämän jälkeen sovellus tarkistaa äänioikeuden. Tarkistuksen perusteella sovellus tarjoaa ne vaalit, joissa äänestäjällä on äänioikeus. Sovelluksen tulee mahdollistaa useampien rinnakkaisten vaalien järjestäminen.

Ohjelmisto olisi käytettävissä vain ennakkoäänestysaikana, koska näin voidaan varmistaa, että vaalipäivänä äänestäminen on aina mahdollista mahdollisista teknisistä ongelmista huolimatta. Mahdollista on myös, että nettiäänestys avautuisi aiemmin kuin ennakkoäänestys ja jatkuisi ennakkoäänestysajan loppuun. Ennakkoäänestysaikana voisi olla mahdollista äänestää uudestaan netin kautta tai korvata nettiääni äänestyslipulla ennakkoäänestyspaikassa. Tällä voitaisiin vähentää mahdollista väärinkäyttöä, toisen puolesta äänestämistä, painostusta tai äänten ostamista. Vaalipäivänä nettiäänestysjärjestelmä ei olisi käytössä, koska näin estetään viimeiseen äänestyspäivään kohdistetun palvelunestohyökkäyksen vaikutukset.

Äänestäjä tekee valintansa käyttöliittymästä. Tyhjän äänestäminen tai äänestyksen keskeyttäminen tulee olla mahdollista. Tämän jälkeen sovellus varmistaa, että valittu vaihtoehto on se, minkä äänestäjä haluaa vahvistaa. Vahvistuksen jälkeen äänestäjä saa kuittauksen, että ääni on viety uurnaan ja että äänestys on siis onnistunut. Käyttäjää tulee informoida kaikista tapahtumista ja varmistaa, ettei käyttäjä kirjaudu ulos

vahvistamatta valintaansa, myöskään silloin, jos käyttäjä haluaa keskeyttää äänestysprosessin.

Päästä päähän varmennettavuus edellyttää, että äänestäjä pystyy äänestämisen jälkeen todentamaan, että hänen äänensä on rekisteröitynyt oikein. Tämä on joissakin nettiäänestysratkaisuissa toteutettu tarjoamalla äänestäjälle mahdollisuus varmistaa äänensä perillemeno äänestyskanavasta riippumattomalla toisella kanavalla. Vahvistusviestin sisältö ja muoto tulee määritellä erikseen, mutta sen tulee tukea vaalisalaisuuden säilyttämistä. Vaalisalaisuuden vuoksi ei voi selväkielisesti palauttaa mitä on äänestetty, mutta jollain tavalla äänestäjän tulee pystyä varmistumaan siitä, että ääni on otettu laskennassa huomioon muuttumattomana.

Nettiäänestyksen äänet säilytetään suojatussa uurnassa identiteettitietojen kanssa ääntenlaskentaan asti. Jos halutaan mahdollistaa uudelleenäänestys nettiäänestyssovelluksessa tai ennakkoäänestyspaikalla paperilla, tulisi äänen ja äänestäjän identiteetin olla linkitettävissä toisiinsa laskentaan asti. Tätä puoltaa myös, se että näin pystytään varmistamaan, että kaikki äänet ovat tallessa ja että uurnassa on vain yksi ääni per äänestäjä. Jos äänten ja äänestäjien lukumäärä poikkeaa toisistaan, selvittäminen on vaikeaa, jos mitään yhteyttä ei ole.

Nettiäänestyksen tulos ei saa olla millään tavalla saatavissa ennen ääntenlaskennan alkua. Ääntenlaskennan alkaessa vaalipäivänä nettiäänet siirretään tuloslaskentaan.

Kansanäänestys

Kansanäänestykset voidaan toteuttaa samalla järjestelmällä kuin vaalit. Ehdokkaiden sijaan sovelluksessa olisi valittavissa äänestettävät vaihtoehdot. Kunnallisiin kansanäänestyksiin käytettävä järjestelmä voidaan myös toteuttaa kevyempänä ratkaisuna, jolloin tietoturvavaatimukset ovat kevyemmät. Kunnallisiin kansanäänestyksiin on lisäksi toteutettava hallintajärjestelmä joko omana järjestelmänään tai osaksi vaalitietojärjestelmää.

Kevennetyillä vaatimuksilla tai kunnallisilla kansanäänestyksissä ei kuitenkaan saada todellisia tuloksia vaalitavan ja teknologian toimivuudesta ja turvallisuudesta, joten tulevaisuudessa toteutetaan kokeilu, niin se on toteutettava oikeissa vaaleissa, esimerkiksi rajatulla äänestäjäjoukolla.

9.2 Lainsäädännön vaatimukset

Nettiäänestyksen käyttöönotto edellyttää vaalilainsäädännön läpikäymistä ja muuttamista nettiäänestysjärjestelmän kehittämistyön rinnalla. Koska kyse on mitä suurimmassa määrin äänestäjän oikeuksista ja velvollisuuksista sekä vaalijärjestelmän toimivuudesta, useista yksityiskohdista tulisi säätää laintasoisesti. Vaalilaissa tulisi säätää nettiäänestykseen oikeutetuista, vaatimuksista äänestäjän tunnistuksen suhteen, nettiäänestyksen ajanjaksosta, nettiäänestysmenettelystä, nettiäänestysjärjestelmän omistajuudesta ja hallinnoinnista sekä toiminnasta poikkeustilanteissa. Todennäköisesti nettiäänestyksen käyttöönotto edellyttäisi myös vaalien muutoksenhakua koskevien säännösten läpikäymistä. Lisäksi tulisi määritellä äänestäjän vastuut vastaavalla tavalla kuin kirjeäänestystä koskevassa hallituksen esityksessä (HE 101/2017 vp).

Nettiäänestysjärjestelmän hallinnointia varten tulisi perustaa uusi vaaliviranomainen, nettiäänestyslautakunta. Nettiäänestyslautakunta voisi koostua puolueiden edustajista vastaavasti kuin vaalipiirilautakunnat. Toisin kuin vaalipiirilautakunnilla, nettiäänestyslautakunnalla olisi toimivaltaa myös kunta- ja maakuntavaaleissa nettiäänestystuloksen vahvistamisessa ja nettiäänestysjärjestelmän hallinnoinnissa kaikissa yleisissä vaaleissa. Nettiäänestyslautakunnan tehtävät ja toimivalta tulisi säätää tarkasti, huomioiden Euroopan Neuvoston suositukset.

Valvonta- ja toimeenpanovastuiden määrittelyssä on varmistettava puolueettomuus ja avoimuus, sekä se ettei vaalijärjestelmä ei voi olla yksinomaan hallituksen tai esimerkiksi turvallisuusviranomaisten hallussa. Nykyisessä vaalilaissa monijäsenisten vaaliviranomaisten (vaalipiirilautakunta, kunnan keskusvaalilautakunta, vaalilautakunta ja vaalitoimikunta) toiminnan puolueettomuutta varmistetaan sillä, että sekä jäsenten että varajäsenten on edustettava aikaisemmissa vaaleissa ehdokkaita asettaneita eri poliittisia ryhmiä. Nettiäänestyksestä vastaavan vaalivalvontaelimen tulisi siis olla vastaavanlainen poliittisen suhteellisuuden ja puolueiden keskinäisen valvonnan mahdollistava toimija.

Virossa on mahdollistettu nettiäänen korvaaminen ennakkoäänestyspaikalla annetulla paperiäänellä. Tällä halutaan turvata äänestystilannetta äänten myymiseltä ja äänestäjän painostamiselta. Nettiäänen korvaaminen toimii kuitenkin myös toisinpäin: äänestäjä äänestää ensin oman tahtonsa mukaisesti, mutta joutuu sitten painostuksesta äänestämään uudelleen. Vaalilaissa tulee linjata, olisiko vastaava menettely mahdollista myös Suomessa. Vaikka moneen kertaan äänestämistä ei sallittaisikaan, lainsäädännössä tulisi määritellä, miten toimitaan tilanteessa, jossa sama äänestäjä on äänestänyt sekä internetin välityksellä ja ennakkoäänestyspaikalla tai esimerkiksi internetin välityksellä ja kirjeellä.

Myös avustajan käyttö tulee linjata nettiäänestyksessä erikseen. Äänestyspaikalla vaaliviranomaiset pystyvät valvomaan avustajan toimintaa ja vaalisalaisuuden toteutumista, mutta valvomattomissa olosuhteissa ei pystytä kontrolloimaan sitä kuka todellisuudessa äänestää. Tunnistusvälineiden luovuttaminen toiselle on kielletty tunnistuslain (617/2009) perusteella, joten tunnistusvälineiden ja tunnistamisen saavutettavuus on varmistettava itsenäisen äänestämisen mahdollistamiseksi.

Vaalilain mukaan vaalien tulos julkaistaan äänestysalueittain. Vaalisalaisuuden turvaamiseksi pienillä äänestysalueilla äänestysalueiden ääniä voidaan laskea yhdessä tai äänestysalueen ennakkoäänet ja vaalipäivän äänet voidaan yhdistää. Vaalilaissa tulisi määritellä, miten turvataan netissä äänestäneiden vaalisalaisuus erityisesti pienillä äänestysalueilla. Mikäli netissä äänestäneitä on vain vähän, nettiäänestyksen tulosta ei voida vaalisalaisuuden vaarantumatta julkistaa erikseen äänestysalueittain.

Vaalilaissa tulisi säätää, että nettiäänestys voidaan jättää ottamatta käyttöön tai keskeyttää sen käyttö vakavassa poikkeustilanteessa. Tällainen säännös sisältyy muun muassa Viron vaalilakiin, mutta sitä ei ole siellä kertaakaan sovellettu. Tällaista tilannetta varten tulee lainsäädännössä määritellä, kenellä olisi päätösvalta nettiäänestyksen poistamisesta käytöstä (todennäköisimmin nettiäänestyslautakunta). Lisäksi tulisi määritellä, miten toimitaan jo annettujen äänten suhteen, jos nettiäänestys joudutaan keskeyttämään kesken ennakkoäänestysjakson.

Nykyiset rikoslain vaalirikossäännökset soveltunevat sellaisenaan myös tilanteeseen, jossa nettiäänestys olisi käytössä. Koska nettiäänestys mahdollistaa paperilla tapahtuvaa äänestystä laajamittaisemman vaaleihin vaikuttamisen, tulisi kuitenkin pohtia, ovatko nykyiset rangaistusasteikot riittäviä tilanteessa, jossa esimerkiksi vallankaappausta yritettäisiin nettiäänestysjärjestelmän manipulointiyrityksen kautta.

Suomessa paperisia äänestyslippuja säilytetään, kunnes seuraavat vaalit on toimitettu. Nettiäänestyksessä lokien tai uurnan säilyttäminen näin pitkään kasvattaa riskiä vaalisalaisuuden murtamisesta, minkä vuoksi esimerkiksi Virossa tiedot tuhotaan heti vaalituloksen vahvistamisen jälkeen. Suomessa vastaavan toimintamallin käyttöönotto edellyttää kuitenkin laajempaa pohdintaa sen suhteen, miten muutoksenhakumahdollisuudet ja vaalisalaisuuden turvaaminen mahdollisimman kattavasti saataisiin toteutettua.

9.3 Vaatimusten määrittely

Kohdearkkitehtuurityöhön kuuluvien vaatimusten tunnistamisen lähteenä on ensisijaisesti käytetty Euroopan Neuvoston tuottamaa suositusta sähköistä äänestystä koske-

vista vaatimuksista. Nämä muodostavat vaatimusmäärittelylle ja sitä seuraavalle tavoiteasetannalle pohjan.

Työssä on pyritty tunnistamaan erityisesti tekniikkaa, luotettavuutta ja tietoturvallisuutta käsitteleviä vaatimuksia, mutta varsinaisen nettiäänestyssovelluksen toiminnallisiin vaatimuksiin ei ole vielä tässä vaiheessa otettu kantaa. Varsinaisen hankintaprosessin käynnistyessä tulee vielä vaatimusmäärittelyä tarkentaa sen verran kuin on tarpeen ja tuottaa rinnalle käyttötapauskuvaukset.

Käytettävyyteen ja saavutettavuuteen liittyvät vaatimukset ovat keskeisiä nettiäänestyssovelluksen käyttöliittymän suunnittelussa ja nämä tulee käydä erityisellä huolella läpi vaatimusmäärittelyä tarkennettaessa.

9.4 Sovellus- ja järjestelmäarkkitehtuuri

Nettiäänestyksen kannalta olennaista on yhtäältä äänestystuloksen oikeellisuus ja luotettavuus sekä toisaalta äänestyssalaisuuden suojaaminen. Arkkitehtuurin kannalta tämä edellyttää äänestystulokseen vaikuttavien annettujen äänien yksikäsitteisen oikeellista käsittelyä sekä järjestelmän korkeaa tietoturvaa. Suunnitellussa arkkitehtuurissa tämä otetaan huomioon hyödyntämällä kahta arkkitehtuurin järjestelmäsuunnitteluperiaatetta:

- Sipuliperiaate (engl. The Onion Principle), jossa toiminnalliset ominaisuudet jaetaan erillisiin alueisiin, jotka on arkkitehtuurissa eriytetty toisistaan.
- Hajautusperiaate, jonka mukaisesti pyritään välttämään suojeltavan tiedon yhteisesitystä, -käsittelyä tai -tallentamista samaan paikkaan.

Sipuliperiaatetta on suunnittelutyössä sovellettu siten, että arkkitehtuuri on jaettu toimialueisiin, joihin on keskitetty toisiinsa loogisesti liittyvät toiminnot. Tavoitteena on, että suojattavat tiedot on mahdollisen tietoturvauhkan kannalta ketjutettu siten, että yhden toimialueen vaarantuminen ei vielä tarkoita koko järjestelmän haavoittuvuutta.

Hajautusperiaatetta on sovellettu erityisesti käyttäjän identiteetin, äänestysoikeuden ja tunnistetun äänestäjän antaman äänen käsittelyssä. Tällä lähestymistavalla pyritään varmistamaan erityisesti äänestäjän identiteetin suojaaminen. Hajautus jakaa identiteetinhallinnan ja äänestysoikeuden varmentamisen kolmeen eri osaan:

Käyttäjän identiteetti tarkistetaan ja vahvistetaan suomi.fi-palvelukokonaisuuden avulla edustajärjestelmässä. Käyttäjään liittyvä äänestysoikeuden auktorisointi tapahtuu

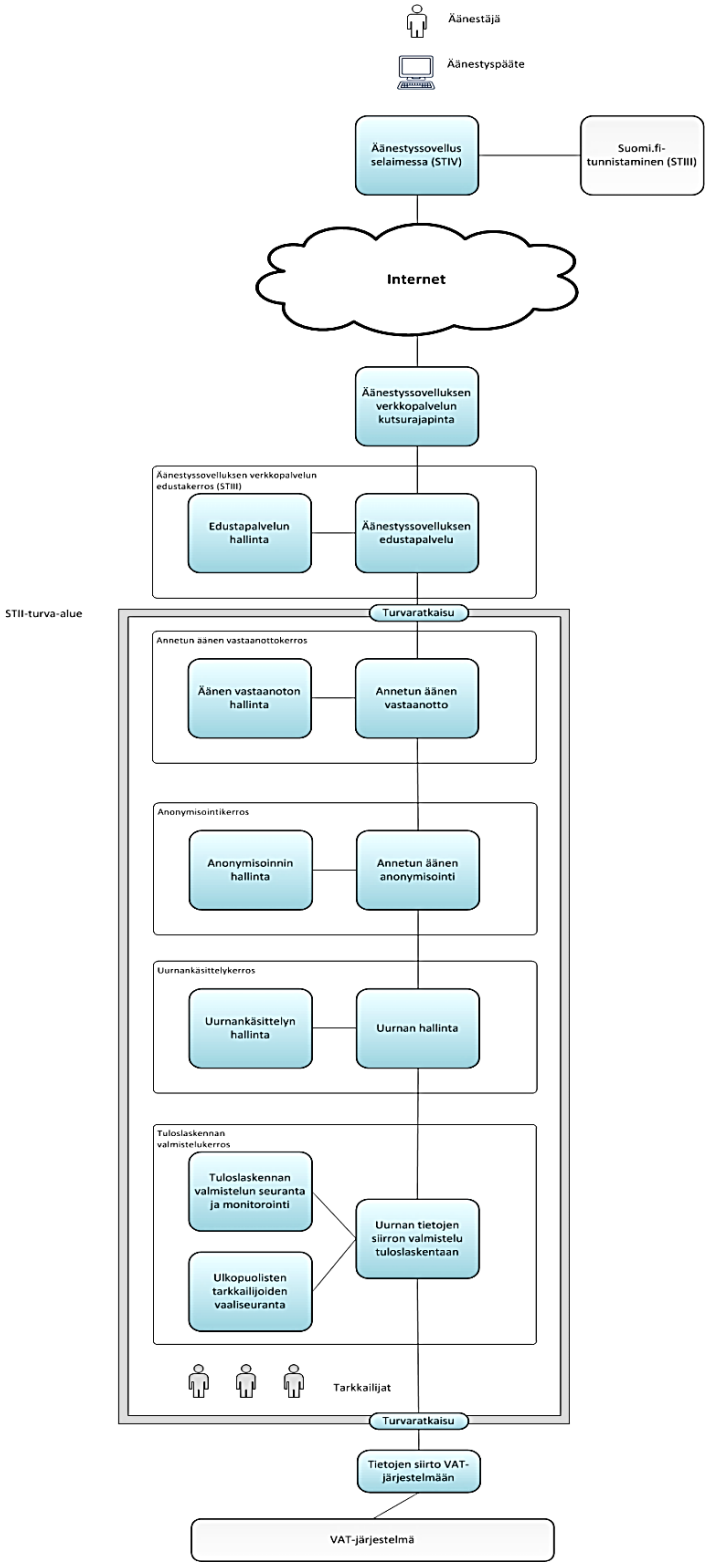
nettiäänestämisen taustajärjestelmässä, joka puolestaan hyödyntää VAT:n äänioikeusrekisteriä. Annetun äänen käsittely tapahtuu vaiheittain nettiäänestämisen taustajärjestelmän eri toimialueissa.

Kukin järjestelmäkokonaisuus on itsenäinen niin toiminnallisessa kuin verkkoavaruuden tarkastelussa. Tällöin mahdollisen tietoturvauhan tulee kohdistua yhtäaikaisesti ja koordinoidusti kaikkiin järjestelmäkokonaisuuksiin (suomi.fi-tunnistaminen, nettiäänestyksen edustajärjestelmä, nettiäänestyksen taustajärjestelmä sekä VAT-kokonaisuus). Toiminnallisesti tällainen koordinoitu hyökkäys on työläs ja kustannusintensiivinen toteutettava.

Esiselvitystyön tuloksena on päädytty suosittamaan arkkitehtuuriskenaariota, jossa nettiäänestysjärjestelmä toteutetaan itsenäisenä sovelluskokonaisuutenaan ja jonka sidokset muihin olemassa oleviin järjestelmiin pyritään minimoimaan mahdollisimman tehokkaasti. Tämän ratkaisun keskeiset ominaisuudet on listattu alla:

NETTIÄÄNESTYSJÄRJESTELMÄN ARKKITEHTUURI

- Tunnistaminen tapahtuu suomi.fi-tunnistamisen avulla.
- Minimoidaan riippuvuudet ulkoisiin järjestelmiin
- Nettiäänestysjärjestelmän edustasovellus toteutetaan mahdollisimman yksinkertaisena
- Eriytetään äänestyssovelluksen rakenne erillisiin toimialueisiin, joiden välinen liikenne on suojattua ja joiden rajapinnat ovat hyvin määriteltyjä.
- Hyödynnetään fyysisen tason arkkitehtuurissa ST2-tason turvamekanismeja äänestystuloksen ja äänestyssalaisuuden kannalta keskeisen tiedon turvaamisessa.
- Suojataan äänestäjän tunnistetietoja samoin kuin annetun ääneen sisältöä äänestyssalaisuuden varmistamiseksi.
- Käyttäjälle tarjotaan äänestyssovellus selainpohjaisena sovelluksena.
- Mahdollistetaan nettiäänestysjärjestelmän edustasovelluksen (front end) ja taustasovelluksen (back end) löyhä riippuvuussuhde.
- Mallinnetaan edustasovelluksen ja taustasovelluksen välinen liikenne hyvin määritellyn ja vahvasti hallitun rajapintakerroksen (ns. API Gateway) avulla.
- Hyödynnetään VAT-järjestelmän tarjoamia palveluita joko sellaisenaan tai hyvin hallituin ja minimoidun muutoksin.



Kuva 5: Nettiäänestysjärjestelmän arkkitehtuuriluonnos

9.5 Järjestelmän sijoittaminen ja ylläpito

Valtiolla on käytössä järjestelmälle sopivia konesalitiloja, joissa samassa kiinteistössä on suojaustasojen II ja III konesaleja ja internet-yhteyksiä. Uurna sijoittuisi tasolle II kuten myös järjestelmän operointitila. Operointitila voidaan rakentaa olemassa olevan huoneen suojaustasoa nostamalla. Pääosa järjestelmän palvelimista sijoittuisi suojaustason III konesaliin.

Järjestelmä tarvitsee ylläpitohenkilökuntaa sekä jatkuvasti että vaalien aikana. Äänestyksen ollessa käynnissä henkilöstön on oltava käytettävissä ympäri vuorokauden. Järjestelmän ytimen ylläpitotehtävien on syytä tapahtua viranomaisten toimesta, edustapalvelinten tiettyjen ylläpitotehtävien ulkoistamista voidaan harkita turvallisuusselvitetyille yritysten työntekijöille. Tarvittavat virat olisi tarkoituksenmukaisinta perustaa Oikeusrekisterikeskukseen. Lisäksi vaalien valvontaan perustettava toimielin tarvitsee käyttöönsä teknistä asiantuntemusta. Tämä asiantuntemus voidaan joko hankkia muista virastoista tai perustamalla toimielimelle tätä varten virka.

Nykyisellä kryptografialla osa äänestysjärjestelmän ylläpitohenkilökunnan operointitehtävistä olisi sellaisia, joissa vaalin tuloksen oikeellisuus tai vaalisalaisuus voisi vaarantua. Tämän vuoksi näiden turvaamiseen on käytettävä muita keinoja. Riskejä tulee hallita arvioimalla kaikki operointitehtävät ja käyttää riskialttiissa tehtävissä, kuten avainten luonnissa, järjestelmän asennuksessa ja tuloksen laskennassa hallittua, valvottua ja usean henkilön toteuttamaa seremoniamenettelyä. Menettelyssä jokainen yksityiskohta suunnitellaan ja harjoitellaan etukäteen, suunnitelma tarkastetaan ja hyväksytään sekä operointitehtävät toteutetaan tarkalla roolijaolla usean henkilön toimesta osan henkilöistä dokumentoidessa jokaisen toimenpiteen ja valvoessa niitä. Tällöin esimerkiksi vaalin tuloksen laskennassa paikalla olisi neljä järjestelmän teknistä ylläpitäjää, kaksi videokuvaajaa, yhdeksän avaimen osan haltijaa, vaalien valvova toimielin, kaksi sihteeriä ja tilaisuuden johtaja. Vastaavaa menettelyä käytetään yleisesti esimerkiksi julkisen avaimen salausjärjestelmien hallinnassa.

9.6 Kustannusarvio

Työryhmä on selvittänyt nettiäänestysjärjestelmän mahdollisia kustannuksia. Kustannusarvio perustuu esiselvitystyön aikana tunnistettuihin vaatimuksiin ja alustavaan arkkitehtuurimalliin. Kustannusarvio on laadittu pääosin arvioimalla hankkeen eri vaiheiden työmääriä sekä henkilötyön ja laitteiston kustannuksia. On myös tavattu mm. konesalipalveluiden tarjoajia.

Kustannusrakenne pitää sisällään hankintavaiheen ja järjestelmän toteutusvaiheen kustannukset. Ensimmäinen käyttöönotto on oma erillinen projektinsa ja tämän jälkeen jokainen järjestettävä vaali tuo omat kustannuksensa. Jatkuvia kuluja näiden lisäksi ovat konesalikustannukset ja ylläpitokulut. Merkittävin osa kustannuksista koostuu tietoturvallisuuden varmistamistoimenpiteistä, kuten tietoturvatarkastuksista, auditoinneista ja fyysisten turvajärjestelyjen varmistamisesta.

Nettiäänestysjärjestelmälle on arvioitu kustannukset 15 vuoden elinkaarelle. Kokonaiskustannusarvio toteutukselle on todennäköisimmän kustannusarvion mukaan 32 miljoonaa (haarukalla 23–40 milj.). Tarkastelujaksolle osuvien vaalien lukumäärä vaikuttaa elinkaarikustannukseen. Kustannuksissa on otettu huomioon hankinta, toteutus, käyttöönotto, viestintä, koulutus, vaalikohtaiset kustannukset sekä vuosittaiset ylläpito- ja konesalikulut.

Kustannusarvio on vasta alustava. Järjestelmäkustannuksiin vaikuttavat merkittävästi mm. tarvittavien resurssien osalta hankintamallin valinta ja markkinatilanne. Nettiäänestysjärjestelmän ytimeksi hankittavan tuotteen käyttöoikeuksien kustannuksien arviointi perustuu vastaavanlaisten hankkeiden julkisuudessa olleisiin summiin.

Työssä arvioitiin myös kustannukset kunnalliseen kansanäänestykseen käytettävälle järjestelmälle. Kokonaiskustannus suomi.fi:n yhteyteen toteutettavalle järjestelmälle on 5,4 miljoonaa. Arvio sisältää hankinnan, ylläpidon ja konesalikustannukset 15 vuoden elinkaarelle.

10 Kilpailutuksen perusteet

10.1 Hankinnan kohde

Nettiäänestysjärjestelmän käyttöönotto vaatii useita erillisiä hankintoja.

1. Nettiäänestyssovellus
2. Ohjelmistokehitys ja auditointi- ja testauspalvelut
3. Laitteisto
4. Konesalipalvelut ST2 & ST3
5. Ylläpito (tarvittaessa)

10.2 Hankintamalli

Nettiäänestyssovellus kannattaa hankkia räätälöitävänä tuotteena, joka kehitetään vaatimusten mukaiseksi sovellustoimittajan ja Oikeusrekisterikeskuksen yhteistyönä. Hankintasopimukseen määritellään ehdot (Proof of Concept), joilla varmistetaan, että sovelluksessa käytettävät teknologiat ja toteutustapa voidaan auditoida ennen lopullista hankintapäätöstä ja toteutusprojektin käynnistämistä.

Käytettävät hankintamenettelyt valitaan, kun nettiäänestysjärjestelmän hankinta on päätetty käynnistää ja tarvittavat periaatteelliset linjaukset on tehty. Tämän jälkeen tarkennetaan vaatimusmäärittelyä ja luodaan käyttötapaukset. Tässä yhteydessä tehdään hankintamenettelyiden valinnat ja nettiäänestyssovelluksen osalta tarvittaessa tarkentava tekninen vuoropuhelu.

10.3 Aikataulu

Hankkeen suunnittelussa tulee ottaa huomioon tulevat vaalit ja mahdollistaa väljä aikataulu, jotta ohjelmistokehityksen jälkeen pystytään testaamaan kokonaisuutta riittävällä laajuudella. Vaalien välissä olevina vuosina pystytään tekemään tarvittavia muutoksia myös vaalitietojärjestelmään. Varsinaisen tuotantotestauksen ja auditointien lisäksi tulee pystyä järjestämään laaja kansalaistestaus lopullisella toteutuksella, jossa saadaan kiinni mahdolliset ongelmat, joita ei ohjelmistotuotannon aikana ole tunnistettu. Tässä on mahdollista tehdä yhteistyötä median kanssa ja toteuttaa kaikille avoin äänestys. Tärkeää on saada massat liikkeelle ja että äänestys toteutetaan teknisesti kuin oikea vaali.

Taulukko 1: Esimerkki aikataulusta

2018	2019	2020	2021	2022	2023
Presidentin-vaalit	Eduskunta-vaalit Europarlament-tivaalit	Ei vaaleja	Kuntavaalit	Ei vaaleja	Eduskuntavaa-lit
Hankepäällikön rekrytointi					
Hankkeen käynnistäminen ja suunnittelu					
	Tarkennettu vaatimus-määritt.				
	Kilpailutusdo-kum. tuottami-nen				
	Kilpailutus				
	Auditointi				
	Hankintapäätös				
	Lainvalmistelu				
		Suunnittelu			
		Ohjelmistokehitys			
			Integrointi		
			Testaukset		
			HE eduskunnal-le, käsittely eduskunnassa	Auditoinnit	
				Laajat käyttäjä-testaukset	
				Koulutus	
				Viestintä	
				Lainsäädäntö voimassa	
					Nettiäänestys käyttöön

11 Yhteenveto

Nettiäänestysjärjestelmä muodostuu kokonaisuudesta, joka pitää sisällään nettiäänestyssovelluksen, edustapalvelun ja taustajärjestelmän. Järjestelmä hyödyntäisi Suomi.fi-tunnistusta, äänioikeusrekisteriä ja vaalitietojärjestelmää. Oikeusministeriö ylimpänä vaaliviranomaisena toimisi kokonaisuuden omistajana ja Oikeusrekisterikeskus vastaisi nettiäänestysjärjestelmän hankinnasta, toteutuksesta ja ylläpidosta.

Jos nettiäänestysjärjestelmän hankinta päätetään käynnistää, sitä ennen tulee linjata seuraavat asiat:

- Mahdollistetaanko uudelleen äänestys nettiäänestyssovelluksessa?
    - Saattaa hankaloittaa äänestäjän painostusta tai äänten myymistä ja turvata osaltaan vaalisalaisuutta
    - Aiheuttaa riskin siitä, että uurnassa olevien nettiäänten salaisuus murretaan, koska edellyttää äänen ja äänestäjän tietojen säilyttämistä yhdessä.
- Voiko nettiäänen korvata paperiäänellä ennakkoäänestyksen aikana tai vaalipäivänä?
    - Vaikeuttaa vaalisalaisuuden varmistamista, koska edellyttää äänen ja äänestäjän tietojen säilyttämistä yhdessä.
- Saako äänestäjä todisteen antamastaan äänestä, miten todiste toimitetaan ja mitä se sisältää?
    - Todiste mahdollistaa vaalisalaisuuden rikkomisen ja äänten myymisen.
    - Vaikeuttaa vaalisalaisuuden varmistamista, koska äänen täytyy olla jäljitettävissä.
- Miten toimitaan, kun syntyy epäily virheestä tai ongelmasta nettiäänestysjärjestelmässä?

Hankintaprosessiin ja lopullisen järjestelmän tarkempaan määrittelyyn tulee osoittaa riittävästi aikaa ja osaamista. Tietoturvallisuus, käytettävyys ja saavutettavuus ovat keskeisiä ominaisuuksia, jotka on otettava huomioon alusta alkaen koko prosessissa. Prosessin avoimuudella voidaan saavuttaa luottamusta ja helpottaa myös mahdollisten ongelmien tunnistamista.

Tunnistuksen osalta on tehtävä periaatepäätös siitä, edellytetäänkö korkean tason tunnistusta eli nykyään käytännössä sähköistä varmennekorttia vai luotetaanko tätä alemmalla tasolla (korotettu taso) oleviin pankkitunnuksiin ja ohjelmallisesti käyttäjän päätelaitteella tuotettuun allekirjoitukseen ja salausavaimeen. Jälkimmäinen vaihtoehto on helpommin käyttöönotettavissa, mutta väärinkäytön riskit ovat siinä suuremmat. Tässä esiselvityksessä työryhmä on selvittänyt eri vaihtoehtojen hyviä ja huonoja puolia. Arvion perusteella nettiäänestysjärjestelmän käytön olisi varminta perustua korkeaan tunnistustasoon mutta haasteena siinä on, että korkean tason tunnistusvälineet eivät ole laajasti käytössä.

Nettiäänestyksellä on haluttu helpottaa muun muassa ulkosuomalaisten äänestämistä, mutta tunnistautuminen ulkomailla vaatii vielä toistaiseksi suomalaiset vahvat sähköiset tunnistusvälineet, joita ei suurella osalla ulkomailla asuvista ole käytössään. eIDAS saattaa tulevaisuudessa helpottaa tilannetta, mutta tämä vaatii vielä useiden vuosien työtä. Pohjoismaiden & Baltian alueella henkilötunnusten hyödyntämistä yli rajojen tullaan selvittelemään lähivuosina.

Päästä päähän varmennettavuuden ja vaalisalaisuuden samanaikainen takaaminen on teknisesti hyvin haastavaa. Äänestäjän tulisi pystyä varmistumaan siitä, että hänen äänensä on siirtynyt laskentaan asti muuttumattomana. On olemassa varteenotettavia nettiäänestysjärjestelmiä, mutta niistä ei mikään täytä vaatimuksia sellaisenaan ja jatkokehityksestäkin huolimatta kokonaistoteutukseen jää riskejä. Lainsäädännöllä ja menettelytavoilla joudutaan paikkaamaan jäljelle jääviä epävarmuuksia. Teknisistä ratkaisuista riippumatta vaalisalaisuus saattaa vaarantua, kun äänestys tapahtuu ilman vaaliviranomaisen valvontaa.

Lohkoketjut mahdollistavat auditoitavan ja hankalasti väärennettävän tapahtumalistan tai lokin ylläpidon. Selvityksessä ei kuitenkaan tunnistettu selkeää hyödyntämistapaa, joka ratkaisisi nettiäänestyksen keskeisiä kysymyksiä.

Nettiäänestysteknologia ja kokonaisuuteen tarvittavien rakenteiden kehittyminen on vielä liian keskeneräistä, jotta järjestelmä voitaisiin toteuttaa ja ottaa käyttöön riittävän turvallisesti. Toteutusteknologiassa on vielä avoimia kysymyksiä vaalisalaisuuden ja varmennettavuuden suhteen. Ei ole nähtävissä, että nettiäänestykseen liittyvät keskeiset riskit ratkeaisivat lähivuosina.

Työryhmä ei suosittele nettiäänestyksen käyttöönottoa, koska tällä hetkellä hankkeen myötä otettavat riskit hyödyt ovat suuremmat kuin hyödyt. Teknologian ja demokratian digitalisoinnin kehitystä tulee kuitenkin seurata tiiviisti ja nykyistä vaalitietojärjestelmää tulee kehittää vastaamaan uusiin vaatimuksiin, jotka ovat syntyneet toimintaympäristön muutosten myötä.

Liite 1: Lainsäädäntö, ohjeet ja standardit

Lainsäädäntö, määräykset, ohjeistukset

Laki		Velvoittavuus
Suomen Perustuslaki	1999/731	Velvoittava
Vaalilaki	1998/714	Velvoittava
Kuntalaki	2015/410	Velvoittava
Arkistolaki	1994/831	Velvoittava
Tilastolaki	2004/280	Velvoittava
Kielilaki	2003/423	Velvoittava
Saamen kielilaki	2003/1086	Velvoittava
Henkilötietolaki	1999/523	Velvoittava
Rikoslaki	1889/39	Velvoittava
Laki julkisen hallinnon tietohallinnon ohjauksesta	2011/634	Velvoittava
Laki viranomaisten toiminnan julkisuudesta	1999/621	Velvoittava
Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta	1999/1030	Velvoittava
Tietoyhteiskuntakaari	2014/917	Velvoittava
Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista	2009/661	Velvoittava
Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä	2013/1226	Velvoittava
Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista	2016/571	Velvoittava
Laki julkisen hallinnon turvallisuusverkkotoiminnasta	2015/10	Velvoittava
Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista	2011/1406	Velvoittava
Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa	2010/681	Velvoittava
Laki julkisista hankinnoista ja käyttöoikeussopimuksista	2016/1397	Velvoittava
Laki julkisista puolustus- ja turvallisuushankinnoista	2011/1531	Velvoittava
Laki neuvoa-antavissa kunnallisissa kansanäänestyksissä noudatettavasta menettelystä	1990/656	Velvoittava
Guidelines on the implementation of the provisions of Recommendation Rec(2017)5 on standards for e-voting	Rec(2017)5	Huomioitava
Sähköisten asiakirjallisten tietojen käsittely, hallinta ja säilyttäminen (SÄHKE2)	AL 9815/07.01.01.00/2008, 19.12.2008	Velvoittava
Määräajan säilytettävien asiakirjojen säilytysajat	989/610/94 OM	Velvoittava
Määräys sähköisistä tunnistus- ja luottamuspalveluista	72/2016	Velvoittava
eIDAS / Komission täytäntöönpanoasetus	(EU) 2015/1502	Velvoittava

Tietoturvallisuus

Ohje tai suositus	Velvoittavuus
OM lokienhallinnan viitearkkitehtuuri	Ohjaava
VAHTI 2/2010 (Ohje tietoturvallisuudesta - hyvä tiedonhallinta- ja tiedonkäsittelytapa)	Ohjaava
VAHTI 3/2012 (Teknisen ympäristön tietoturvataso-ohje)	Ohjaava
Kansalliset kryptografiset vahvuusvaatimukset	Ohjaava
VAHTI 12/2006 (Verkkopalvelut)	Ohjaava
VAHTI 2/2015 (Ohje salauskäytännöistä)	Ohjaava
VAHTI 9/2008 (Hankkeen tietoturvaohje)	Ohjaava
VAHTI 3/2009 (Lokien käsittelyohje)	Ohjaava
VAHTI 3/2011 (Valtion ICT-hankintojen tietoturvaohje)	Ohjaava
VAHTI 2/2016 Toiminnan jatkuvuuden hallinta	Ohjaava
Kansallinen turvallisuusauditointikriteeristö (versio 3)	Ohjaava
VAHTI 1/2013 Sovelluskehityksen tietoturvaohje	Ohjaava
JHS 167 Neuvottelumenettelyjen käyttö ICT-hankinnoissa	Huomioitava
JHS 169 Avoimen lähdekoodin ohjelmien käyttö julkisessa hallinnossa	Huomioitava
JHS 174 ICT-palvelujen palvelutasoluokitus	Huomioitava
JHS 182 ICT-palvelujen kehittäminen: Laadunvarmistus	Huomioitava
JHS 190 Julkisten verkkopalvelujen suunnittelu ja kehittäminen	Huomioitava
JHS 198 Kokonaisarkkitehtuurin peruskuvaukset	Huomioitava
Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting	Ohjaava
Handbook for the Observation of New Voting Technologies (Organization for Security and Co-operation in Europe)	Ohjaava

Velvoittavan sidosarkkitehtuurin velvoittavuus perustuu pääasiallisesti julkisen vallan käytössä ilmaistuun normiin, jota on tyypillisesti noudatettava virkavastuun uhalla. Tällaisia velvoittavia lähteitä ovat lait ja niiden antaman valtuutuksen nojalla edelleen annetut asetukset sekä alemmanasteiset säädökset. Tyypillisesti velvoittavat sidosarkkitehtuurit eivät sisällä poikkeusmenettelyä, ellei jokin olemassa oleva vastaavantasoinen normi anna siihen mahdollisuutta.

Ohjaava sidosarkkitehtuuri sisältää arkkitehtuurilinjauksia, joita pyritään noudattamaan. Noudattamisesta on mahdollisuus kuitenkin harkinnanvaraisesti poiketa, jos siihen löytyy perustellut syyt ja noudattamisesta koituisi kohtuutonta haittaa. Poikkeamat ohjaavista sidosarkkitehtuureista hyväksytään kokonaisarkkitehtuurin hallintamallin mukaisella päätöksentekoprosessilla.

Huomioitavan sidosarkkitehtuurin vaikutuksia seurataan jatkuvasti ja niistä voidaan hakea valmiita ratkaisutapoja ja -malleja arkkitehtuurityöhön, mutta niiden noudattamiseen ei ole tunnistettu syntyvän velvoittavuutta. Hyviä esimerkkejä huomioitavista sidosarkkitehtuureista ovat tekniset standardit, alan parhaat käytänteet ja meneillään olevat rinnakkaiset kehittämisprojektit.

OIKEUSMINISTERIÖ JUSTITIEMINISTERIET

ISSN 1798-7091 (nid.)
ISSN 1798-7105 (PDF)
ISBN 978-952-259-660-4 (nid.)
ISBN 978-952-259-661-1 (PDF)

Oikeusministeriö
PL 25
00023 Valtioneuvosto
www.oikeusministerio.fi

Justitieministeriet
PB 25
00023 Statsrådet
www.justitieministeriet.fi