Nettiäänestyksen esiselvitys
22.9.2017

Esiselvitys

- Toimeksianto: Työryhmän tulee laatia Julkisen hallinnon tietohallinnon neuvottelukunnan suosituksen JHS 172 ”ICT-palvelujen kehittäminen; Esiselvitys” mukainen selvitys yleisissä vaaleissa ja neuvoa-antavissa kansanäänestyksissä käytettävästä nettiäänestysjärjestelmästä.
- Työssä on
  - pyritty löytämään ne vaatimukset, joilla järjestelmä voidaan toteuttaa nykytilanne ja tunnistetut riskit huomioiden
  - tutustuttu markkinakartoituksen kautta Euroopassa käytössä oleviin vastaaviin järjestelmiin
  - pohdittu hankintavaihtoehtoja
  - tunnistettu kysymyksiä, jotka tulisi ratkaista, ennen kuin lopullinen päätös toteutushankkeesta voidaan tehdä
  - Tehty karkea kustannusarvio, joka tarkentuu työn edetessä

Tunnistetut periaatteet

1. Eheys (vaalisalaisuuden kanssa vaikea toteutettava)
2. Vaalisalaisuus (eheyden takaamisen kanssa vaikea toteutettava)
3. Äänestäjän autentikointi > Äänioikeus
4. Saatavuus
5. Saavutettavuus
6. Ymmärrettävyys > Luotettavuus

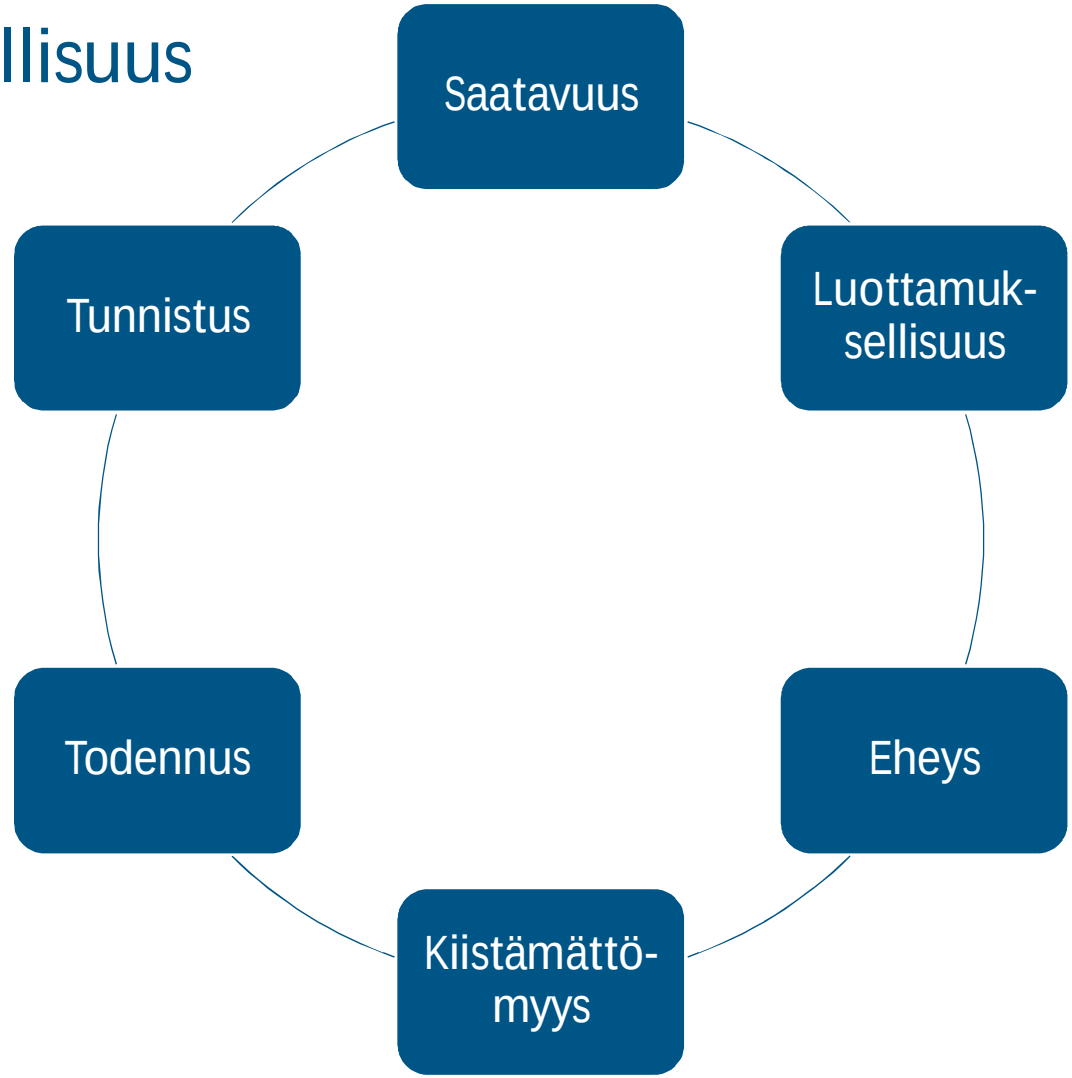
Suunnittelun tavoitteet

1. Äänestyksen turvallisuus ja luotettavuus.

2. Äänestysjärjestelmän käytettävyys ja käyttökelpoisuus.

3. Äänestysprosessin luotettavuus ja läpinäkyvyys.

Tietoturvallisuus



Tietoturvariskien kartoitus

- Tietoturvariskien kartoituksen toteutti F-Secure
- Työpajoihin osallistui edustajia seuraavista organisaatioista: oikeusministeriö, Oikeusrekisterikeskus, keskusrikospoliisi, puolustusvoimat, Valtori, Viestintävirasto, valtioneuvoston kanslia
- Selvityksessä tunnistettiin riskit, niiden vaikutukset ja esitettiin mahdolliset hallintakeinot, joista johdettiin vaatimuksia järjestelmälle

Vakavimmiksi riskeiksi tunnistettiin

1. Vaalituloksen laaja manipulointi
2. Vaalien häirintä palvelunestohyökkäyksillä
3. Vaalisalaisuuden murtuminen aiheuttaa epävakautta

Markkinakartoitus

Tutustuttiin tarkemmin kahteen käytössä olevaan nettiäänestysjärjestelmään: Scytl (Sveitsi, Ranska, Norjan kokeilu), Cybernetica (Viro)

- Vastausten perusteella ei kumpaakaan toimittajaa ei ole perusteltua sulkea pois mahdollisena nettiäänestysjärjestelmän toimittajana Suomen yleisiin vaaleihin
- Esiselvityksen riskikartoituksessa esiin tuotuja merkittävimpiä riskejä ei voida kuitenkaan 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 vaatimuksista, jotta jokin toinen vaatimus tulisi mahdolliseksi. Nämä päätökset ovat todennäköisesti poliittisia.

Markkinakartoitus

Toimittajien ratkaisut koskevat äänestämisen järjestämisen osaongelmia, eivätkä itsessään ole valmiita avaimet käteen –ratkaisuja

- Toimittajien ratkaisuilla äänien eheä toimitus koko matkalla äänestäjältä vahvistettuun tulokseen ei toteudu
- Kokonaisvastuu auditoinnin ja monitoroinnin toteutuksesta, seurannasta ja hälytyksistä olisi meillä
- Dokumentaation ja lähdekoodin avoimuus ei ole itsestään selvää
- Toimittajien suhtautumisessa tietoturvaan ohjelmistokehitysprosessissa on toimittajakohtaisia eroja, jotka voivat vaikuttaa tuotteen turvallisuuteen
- Varsinaisessa hankintaprosessissa on varattava riittävästi aikaa tuotteiden turvallisuusominaisuuksien auditointiin

Todennäköisin toteutusskenaario

- Nettiäänestys olisi osa nykyistä vaalitietojärjestelmää
- Nettiäänestyssovellus hankittaisiin tuotteena
- Jatkokehitys/räätälöinti ja järjestelmän rakentaminen tehdään tunnistettujen vaatimusten mukaisesti
- Hyödynnetään suomi.fi -palveluita: portaali, tunnistautuminen
- Omistajuus oikeusministeriöllä, kirjattava lakiin
- Keskitetty nettivaaleja valvova elin
  - Toimeenpano- ja valvontavastuissa huomioitava puolueettomuus
  - Parlamentaarinen valvonta myös vaalien aikana

Eheys vs. vaalisalaisuus

Tapahtumien jäljitettävyys

Nettiäänestyksen eheyden varmistaminen edellyttää, että kaikista äänestämiseen ja järjestelmän ylläpitoon liittyvistä tapahtumista jää turvallisesti säilytettävät tapahtumalokit. Lokien osuus on keskeinen mahdollisten virheiden ja väärinkäytösten tutkinnassa. Mutta vaikka tarkat lokikirjaukset ovat keskeisiä äänestystuloksen eheyden varmistamiseksi, ovat ne mahdollinen riskilähde vaalisalaisuuden paljastumiselle .

Uudelleenäänestyksen mahdollisuus

Nettiäänestyksen yhteydessä tapahtuvaa painostamista tai äänesten myyntiä voidaan rajoittaa mahdollistamalla nettiäänen antaminen uudelleen ennakkoäänestysajan puitteissa. Tällöin painostus tai ostaminen olisi tehokasta vain, jos se olisi mahdollista tehdä hyvin lähellä ennakkoäänestysajan päättymistä.

Hallintakeinon toteuttaminen tarkoittaa, ettei sähköisesti annettuja ääniä voida sekoittaa heti niiden antamisen jälkeen. Sähköisesti aiemmin annettu ääni on pystyttävä poistamaan uurnasta. Tämä lisää riskiä sille, että äänet yhdistetään luvattomasti äänestäjiin.

Eheys vs. vaalisalaisuus

Mahdollisuus antaa ääni vaalipäivänä

Nettiäänestyksen yhteydessä tapahtuvaa painostamista tai äänten myyntiä voidaan rajoittaa mahdollistamalla nettiäänen korvaaminen vaalipäivänä annetulla äänellä. Uhkatoimijan tulisi tällöin varmistaa, etteivät hänen painostamansa tai lahjomansa henkilöt pääse äänestämään tuona päivänä. Tämän toteuttaminen suuressa mittakaavassa on vaikeaa ja teko on nykyisellään määritelty rikokseksi (vaalirikos).

Hallintakeinon toteuttaminen tarkoittaa myös, ettei sähköisesti annettuja ääniä voida sekoittaa heti niiden antamisen jälkeen. Sähköisesti aiemmin annettu ääni on pystyttävä poistamaan uurnasta. Tämä lisää riskiä sille, että äänet yhdistetään luvattomasti äänestäjiin.

Äänen varmistaminen toisesta kanavasta

Nettiäänestysjärjestelmään on mahdollista yhdistää toimintoja, joiden avulla äänestäjä voi tarkistaa, kenelle hänen äänensä on rekisteröity. Tällä keinolla on mahdollista lisätä luottamusta ja läpinäkyvyyttä nettiäänestämiseen.

Hallintakeinon toteuttaminen tarkoittaa, ettei sähköisesti annettuja ääniä voida sekoittaa heti niiden antamisen jälkeen. Tämä lisää riskiä sille, että äänet yhdistetään luvattomasti äänestäjiin.

Äänen tarkistaminen tarkoittaa käytännössä myös datan siirtämistä ulos suojatusta ympäristöstä esimerkiksi sähköpostiin tai mobiiliverkkoon. Varsinaista äänen sisältöä ei viestissä voida tuoda, mutta tieto yleensä siitä, että ääni on tallessa voisi olla mahdollinen.

Vaalisalaisuus ja pienet äänestysalueet

Jos äänestysalueella on 63 §:n mukaisesti hyväksyttyjä vaalikuoria vähemmän kuin 50 tai jos voidaan perustellusti arvioida, että äänestysalueella äänestää vaalipäivänä vähemmän kuin 50 henkilöä, kunnan keskusvaalilautakunnan on määrättävä, että äänestysalueen ennakkoäänet ja vaalipäivän äänet lasketaan yhdessä. Tällöin äänestysalueen vaalilautakunta ei suorita vaalipäivän äänten alustavaa laskentaa, vaan toimittaa äänestysliput alustavaa laskentaa varten keskusvaalilautakunnalle.

- Nettiäänestyssovelluksessa tulee siis olla mahdollisuus yhdistää 1 tai useampi äänestysalue toisiinsa näissä tapauksissa. Tällöin myös vastaavat tulee yhdistää paperiäänten laskennassa.
- Vaalilaissa huomioitava

Tunnistus

- Nettiäänestysjärjestelmän sisältämän tiedon tietoturvallisuusvaatimus on korkea. On pystyttävä estämään henkilöllisyyden väärinkäyttö ja muuttaminen.
- Tämä tarkoittaa käytännössä vahvaa sähköistä tunnistusta, joka on luokitukseltaan korkea.
- Korkealle tasolle pääsevät tällä hetkellä vain VRK:n myöntämät varmennekortit, mutta tilanne voi muuttua tulevaisuudessa.

Sähköinen henkilökortti	690 000 kpl
Sosiaali- ja terveydenhuollon ammattikortit	235 000 kpl
Organisaatiokortit	70 000 kpl

Kaikkiin muihin kansalaisten sähköisiin palveluihin riittää pankkitunnukset

Vertailu

	Korotettu	Korkea
Tunnistusvälineet	Esim. pankkitunnukset	Varmennekortti
Käyttäjät	Käytännössä kaikilla suomalaisilla, joilla tili suomalaisessa pankissa	Sähköinen henkilökortti 690 000 Soster 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

Seuraavaksi

- Kustannusarvion tarkentaminen
- Hankintavaihtoehtojen tarkentaminen
- Etenemissuositukset

- Käydään läpi parlamentaarisessa seurantaryhmässä
  - Työryhmä työstää esiselvityksen ja loppuraportin valmiiksi

- Tavoiteaikataulu: marraskuun loppu

Parlamentaarinen seurantaryhmä

- 25.10. klo 8-9.30
- Etenemissuositusten läpikäynti

Työryhmä

- 30.10. klo 13-15
- Aineistojen läpikäynti ja eteneminen