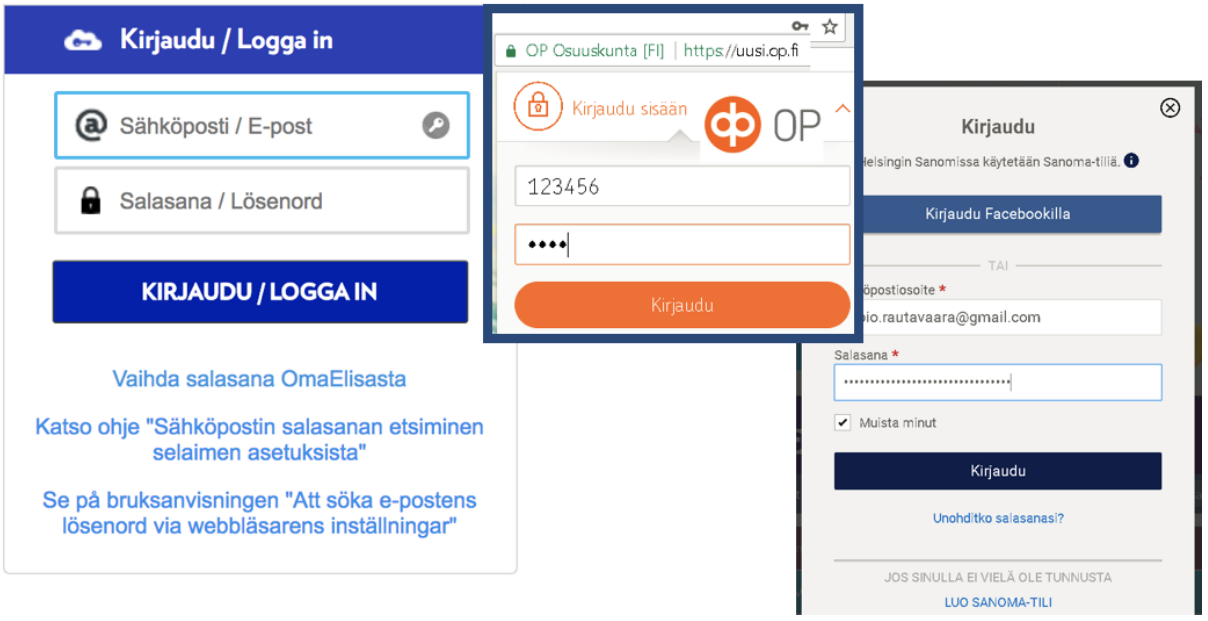
KIRJAUTUMINEN JA TUNNISTAUTUMINEN SÄHKÖISISSÄ PALVELUISSA



Työryhmä: ENTER ry:n vertaisopastajat Ilkka Liedes, Esa Martonen,

Kari Pulkkinen, Mårten Stenius, Ilkka Veuro

Huhtikuu 2018

enter
Ikäihmisten tietotekniikkayhdistys

TUETTU VEIKKAUKSEN TUOTOILLA

Sisällysluettelo

1. Kirjautuminen sähköisiin palveluihin 3

1.1 Erilaiset palvelut moneen tarkoitukseen 3

1.2 Palveluiden luokittelu 4

1.3 Tunnistautumisratkaisut 5

1.4 Pankkipalvelut 7

2. Salasanojen luonti ja käyttö 7

2.1 Hyvä salasana 7

2.2 Salasanojen tallentaminen 8

2.3 Unohtunut salasana (palauttaminen) 9

2.4 Sähköpostin salasanan merkitys - identiteettivarkaus 10

3. Tunnistautuminen julkishallinnon palveluihin 10

3.1 Yhtenäinen ratkaisu 10

3.2 Suomi.fi -tunnistautuminen 11

3.2.1 Varmennekortti 12

3.2.2 Mobiilivarmenne 12

3.2.3 Pankkitunnisteet 13

4. Muita kirjautumistapoja: oikoteitä tai lisäturvaa 13

4.1 Tunnistautuminen Facebook- tai Google-tunnuksilla 13

4.2 Kaksivaiheinen kirjautuminen 14

4.3 Sovellussalasanat 16

5. Mobiililaitteen vaihto 16

6. Kirjautumisilmoitukset ja varoitukset 17

6.1. Ilmoitusten tarkoitus 17

6.2. Esimerkkitapaukset 17

6.2.1 Microsoft 18

6.2.2. Google 19

6.2.3. Facebook 22

6.2.4. Apple 24

6.3. Huijaukset 25

Liite 1: Suomi.fi -sisällöstä tarkemmin 26

Liite 2: Varmennekortista tarkemmin 27

Liite 3: Mobiilivarmenteesta tarkemmin 30

1. Kirjautuminen sähköisiin palveluihin

1.1 Erilaiset palvelut moneen tarkoitukseen

Palveluja ovat esimerkiksi käyttäjätilit, sähköpostit, sähköiset pankkipalvelut, sosiaalisen median (some-) palvelut, verkkokaupat, operaattorien palvelut, kirjastojen sähköiset palvelut jne. Yhteistä palveluille on, että ne edellyttävät kirjautumista käyttäjätunnuksella ja salasanalla. Nykyisin vain harvat palvelut käyttävät muunlaista käyttäjätunnusta kuin sähköpostitunnusta. Sähköpostitunnuksen käyttäminen käyttäjätunnuksena helpottaa myös palveluun kirjautumista.

Käyttäjätunnusta luodessa kannattaa palveluun tallentaa unohtuneen salasanan palautusta varten puhelinnumero tai toinen sähköpostiosoite. Näiden mahdollisuuksien puuttuessa palautuksessa voi käyttää ennalta annettuja kysymys-vastaus -pareja.

Esimerkkejä käytetyimmistä palveluista:

Sähköposti(t) - gmail.com, inet.fi, elisa.fi, outlook.com, suomi24.fi, welho.com, luukku.com, kolumbus.fi, saunalahti.fi

- sähköposti on keskeinen tekijä, kun henkilö haluaa käyttää sähköisiä palveluja ja/tai osallistuu ns. digiyhteiskuntaan. Sähköpostissa henkilö valitsee itselleen sähköpostitunnuksen ja salasanan, jonka laatua sähköpostipalvelun tarjoaja saattaa valvoa. Sähköpostitunnus on usein muotoa “etunimi.sukunimi@sähköpostipalvelu.fi” tai .fi:n tilalla .com. Sähköposti mahdollistaa myös viestien lähettämisen ja vastaanottamisen muille sähköpostia käyttäville.
- sähköpostitunnusta käytetään nykyisin useimpien palveluiden käyttäjätunnuksena
- voi käyttää valikoiden kahta tai kolmea sähköpostiosoitetta eri palveluihin sekä unohdetun salasanan palautustarkoituksiin

Pankki

- käyttäjätunnus, salasana ja/tai pankin toimittama avainlukulista/tunnuslukukortti/tunnuslukusovellus

- palauttaminen pankin konttorissa tai asiakaspalvelun kautta

Käyttäjätilit: Microsoft, Google, Apple ja iCloud

- sähköpostitunnus ja salasana
- sovellusten hankinta laitteen sovelluskaupasta
- käytetään myös laitteiden aktivointiin
- ERITTÄIN tärkeää tallentaa salasanan palautusta varten puhelinnumero
- muita käyttäjätilejä esim. Dropbox, Samsung jne.

Somepalvelut: Facebook, Instagram, YouTube, LinkedIn

- sähköpostitunnus ja salasana
- salasanan palautus puhelinnumerolla

Muita käyttäjätilejä, joissa sähköpostitunnus toimii käyttäjätunnuksena

- Verkkokaupat (Zalando, Amazon, ..)
- Operaattorit, Yle-tunnus, hs.fi, sähköyhtiöt…
- Laite- ja ohjelmistotoimittajien rekisteröinti

Kirjastojen Helmet palvelussa käyttäjätunnuksena on kirjastokortin numero ja salasanana kortin PIN-koodi.

Turvakysymykset (kysymys-vastaus -parit)

- kirjoita kysymykset ja vastaukset talteen (huom isot ja pienet kirjaimet ovat eri merkkejä)

1.2 Palveluiden luokittelu

Luokittele palvelut niille asettamiesi **omien** tietoturvavaatimustesi mukaan

- tärkeitä esim. Google, Apple ja Microsoft, joihin palveluiden lisäksi liittyy puhelimen, tabletin tai tietokoneen käyttöönotossa tarvittava käyttäjätili. Erityisen tärkeitä palveluita ovat mm. pankki, PayPal ja muut, joihin on talletettu maksutietoja. Muita tärkeitä ovat palvelut, joihin on talletettu henkilökohtaisia tietoja esim. Facebook, LinkedIn, Instagram, operaattoritunnukset

- vähemmän tärkeitä esim. uutiskirjetilaukset, Yle, Iltalehti, kirjoittimen laiterekisteröinti

On mahdollista luoda useampia sähköpostitunnuksia (myös eri palveluntarjoajille) ja käyttää niitä valikoivasti eri palveluissa.

Vaikka samaa sähköpostitunnusta käyttää useassa palvelussa, voi eri palveluille luoda luokituksen mukaisesti omat salasanat.

- Kaikille tärkeille palveluille tulee luoda yksilöllinen salasana joka palvelulle.
- Tärkeiden palveluiden salasanaa ei suositella tallennettavan selaimeen.
- Vähemmän tärkeissä palveluissa voi käyttää myös samoja salasanoja oman harkinnan mukaan.

Jos jossain palvelussa pitää vaihtaa salasanan, pitää vaihto tehdä myös kaikissa käytössä olevissa laitteissa (tietokone, puhelin ja tabletti).

Teleoperaattoreiden sähköposteissa on huomattava, että joskus ne voivat olla kytköksissä operaattorin myymään liittymään. Jos vaihdat liittymän toiselle operaattorille, voi sähköposti muuttua maksulliseksi.

1.3 Tunnistautumisratkaisut

Rajoitetulle henkilöjoukolle tarkoitetut palvelut tai laitteet vaativat pääsyoikeuden mahdollistamiseksi käyttäjän tunnistautumisen.

Pääsyoikeuden saanti voi vaatia joko heikon tai vahvan tunnistautumisen. Kaikki mikä ei ole vahvaa tunnistautumista, on heikkoa tunnistautumista. Vahva tunnistautuminen nojautuu kahteen tai useampaan todentamistapaan. Usein käytössä on käyttäjätunnus ja salasana, joiden lisäksi toisena todentamistapana voidaan käyttää esimerkiksi seuraavia ratkaisuja:

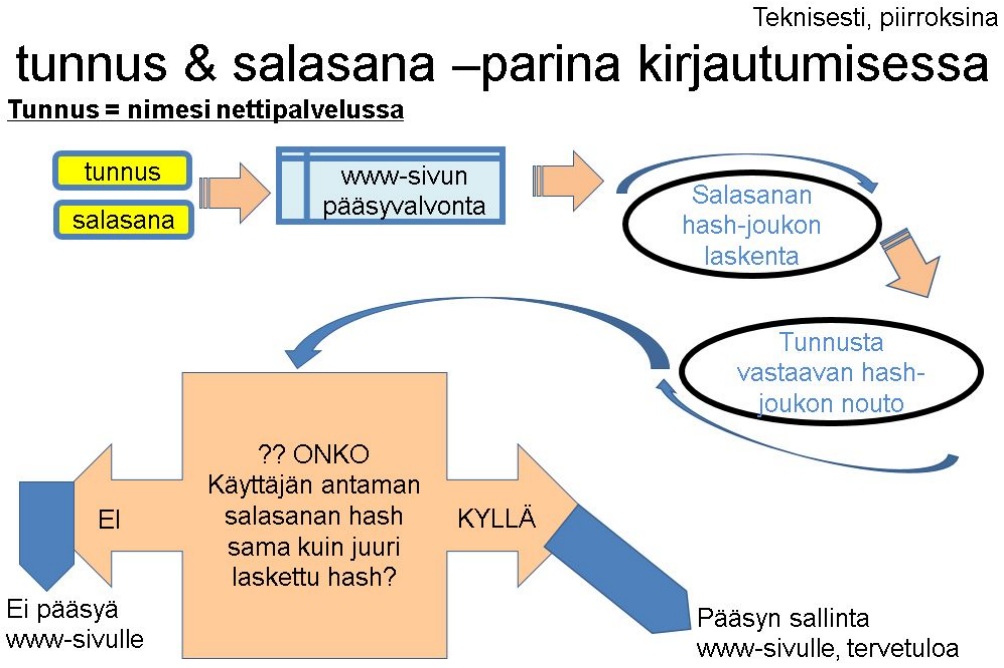
- Toimikortti, esim. henkilökortin ns. kansalaisvarmenne mikropiirissä ja sen avaamisen salanumero

- Mobiilivarmenne puhelimessa
- Tunnetut, luotettavaksi todetut kansalliset tunnistuspalvelut. Esim. tunnistautuminen pankkiyhteydellä asiakasnumero ja laite (kuten avainlukutaulukko, tunnuslukulaite tai tunnusluvun lähettävä sovellus kuten Nordea-tunnuslukusovellus)
- Muu tunnusmerkit täyttävä tekninen ratkaisu, esimerkiksi matkapuhelimeen tuleva tekstiviesti tai puhelu, joka edellyttää yleensä lisäksi käyttäjän tunteman PIN-koodin syöttämistä

Heikossa tunnistautumisessa käytetään yleensä vain käyttäjätunnus & salasana -paria. Salasanan vaatimukset ovat palvelusta riippuvia (vähimmäismerkkimäärä, pienet/isot kirjaimet ja erikoismerkit).

Käyttäjätunnus ja salasana ovat pari. Käyttäjätunnus tallennetaan selväkielisenä palvelun hallinnoinnin tietoihin, mutta salasana ei ole selväkielisenä vaan sekasummana (hash). Näin hallinto ei voi antaa salasanaa, mutta voi vaihtaa salasanan kertoen muutetun salasanan turvallisella tavalla.

Teknisesti, piirroksina



1.4 Pankkipalvelut

Pankkipalveluihin kirjaudutaan käyttäen kunkin pankin omaa vahvaa tunnistautumista. Turvallisinta on käyttää puhelimella tai tabletilla kunkin pankin omaa mobiilisovellusta, vaikka pankkipalveluita voi käyttää myös nettiselaimen kautta. Mobiilisovelluksen yhteys pankkiin on aina varmistettu.

Mobiilisovelluksen vaihtoehtona useimmat pankit tarjoavat käyttöön ns. tunnuslukulaitteen joka on pienen laskimen kokoinen. Tästä käytetään myös nimitystä PIN-koodilaite (PIN code generator).

Käytettäessä nettiselainta tulee varmistaa, että yhteys on suojattu (osoiterivillä https tai lukkosymboli) ja että tietoturva on ajan tasalla.

Lukkosymboli osoiterivillä kertoo suojatusta yhteydestä.

2. Salasanojen luonti ja käyttö

2.1 Hyvä salasana

Vaatimukset hyvälle salasanalle ovat muuttuneet ajan ja etenkin tietokoneiden laskentatehon nopean kasvun myötä. Pitkään on ajateltu, että isojen ja pienten kirjainten sekä numeroiden sekoittaminen lisättynä erikoismerkeillä tekee salasanasta laadukkaan. Useat palvelut eivät edes hyväksy muunlaisia salasanoja. Nykyisen tiedon valossa hyvän salasanan keskeinen vaatimus on, että se on riittävän pitkä, ei muodostu yhdestä sanasta eikä koostu pääosin numeroista ja/tai erikoismerkeistä.

Vaatimuksia:

- vähintään 15 merkkiä
- suositaan kirjaimia (tulee enemmän vaihtoehtoja)
- helppo muistaa, mutta vaikea arvata
    - EI: lasten tai lemmikin nimi, kotikaupunki
    - KYLLÄ: kolmen sanan yhdistelmä tai lause voi olla helppo muistaa esim. muistisäännöllä

- helppo kirjoittaa virheettömästi, salasanan joutuu kirjoittamaan sokkona
- useimpiin vaaditaan isoja ja pieniä kirjaimia, numeroita ja joskus myös erikoismerkkejä
    - ei kuitenkaan kannata käyttää ääö tai muita erikoisia kirjaimia
    - eikä aksenttimerkkejä, “:”, “”, “’”, …
- vaikea hakkeroida
    - EI: yksittäinen sana, nimi, numerosarja, syntymäaika (oma/omaisen), puhelinnumero

Esimerkkejä salasanoista ja kuinka nopeasti hakkerit voivat murtaa sen:

- Tampere - alle 1 s
- TampereAamulehti - 1 v
- TampereAamulehti2018 - yli 100 v
- koivu - alle 1s
- koivu-haapa - 1 pv
- koivu-haapa-kuusi - yli 100v

Salasanan turvallisuuden voi testata täällä: https://yle.fi/aihe/artikkeli/2017/02/01/digitreenit-17-salasanakone-testaa-kuinka-nopeasti-salasana-murretaan

2.2 Salasanojen tallentaminen

Kuten aikaisemmin on kerrottu, yhdellä salasanalla ei pärjää palveluiden ja tilien kirjossa. Jotta muistaa kaikki eri palvelut ja niiden eri salasanat, ne on talletettava jonnekin, mistä ne tarvittaessa löytää.

Helpoin ja yksinkertaisin tapa on kirjoittaa palvelu ja sen salasana talteen *paperivihkoon*, jota säilyttää normaalisti kotona turvallisessa paikassa. Tullessa opastuspalveluun vihko on otettava mukaan. Lisäksi pitää muistaa salasanaa vaihtaessa viivata yli vanha salasana ja kirjoittaa vihkoon uusi. Tämä tahtoo helposti unohtua. Vihko on huomattavasti parempi kuin epämääräinen kasa lippuja ja lappuja.

Toinen helppo tapa on tallentaa salasanat *selaimeen*. Selaimissa ainakin Chrome ja Safari myös synkronoivat kirjautumistiedot kaikkiin laitteisiin, joissa samaa selainta

käytetään. Salasanojen tallentaminen selaimiin on suositeltavaa lukuun ottamatta tärkeitä palveluita.

Salasanasovellukset ovat myös hyvä tapa säilyttää salasanoja. Nämä sovellukset tietysti myös vaativat oman salasanan, jota ei sitten kannata unohtaa, päästäkseen hallitsemaan salasanoja. Usein näihin sovelluksiin voi turvallisesti tallettaa myös muita tietoja kuten sosiaaliturvatunnuksia tai luottokorttinumeroita ja niiden PIN koodeja. Näitä ohjelmia on sekä maksuttomia että maksullisia. Maksuttomat toimivat yleensä yhdessä laitteessa ja maksulliset synkronoivat salasanat kaikkiin laitteisiin.

Salasanoja tai PIN-koodeja ei suositella talletettavan osoitekirja-, muistiosovelluksiin tai pilvitiedostoon. Jos näin tehdään on oltava tarkkana, että ei kirjoita tietoja liian helposti löydettäväksi, jos vaikkapa joku varastaa tai kaappaa laitteen tai laitteen varmuuskopion.

2.3 Unohtunut salasana (palauttaminen)

Salasanan unohtaminen tai hukkaaminen on silloin tällöin tapahtuva ilmiö. Salasanan palautuksen menettely vaihtelee kovasti eri palveluissa.

Muutamissa yleisissä palveluissa ei ole olemassa mitään asiakaspalvelua (esim. Google), vaan palautus tapahtuu täysin itsepalvelua. Jos salasanaa ei saa itse palautettua, on henkilön pakko tehdä uusi tunnus tähän nettipalveluun ja tällöin ei vanhoihin tietoihin enää pääse käsiksi.

Yksinkertaisimmillaan salasanan palautus toimiii nettisivulla syöttämällä käyttäjätunnuksensa (sähköpostinsa tai puhelinnumeronsa) ja klikkaamalla palautuslinkkiä (esim. *Unohditko salasanasi?*). Sen jälkeen saat sähköpostiisi linkin, jonka kautta voi luoda uuden salasanan.

Google, Apple tai Microsoft-tilin palautus toimii sujuvimmin tunnistautumalla palveluun talletetun puhelinnumeron avulla. Käyttäjä saa puhelimeensa tekstiviestinä kertakäyttöisen numerokoodin, jolla varmistetaan käyttäjän henkilöllisyys. Tämän vuoksi käyttäjätiliin pitää aina laittaa oma puhelinumero. Sillä, onko puhelin perusmallia vai älypuhelin, ei ole merkitystä.

2.4 Sähköpostin salasanan merkitys - identiteettivarkaus

Sähköposti toimii usein tärkeänä kohteena tehtäessä identiteettivarkautta. Urkitun salasanan avulla varastetaan kohteen sähköpostitili ja muutetaan sen salasana. Sen jälkeen henkilön sähköposteista selvitetään, mihin palveluihin hän (= kohde) on kirjautunut. Sitten varas käyttää palveluissa ‘Unohtuiko salasana’ -toimintoa, jolla saadaan muutettua palvelun salasana. Tällä tavalla päästään kaikkiin kohteen palveluihin käsiksi. Varkauden kohde ei itse pysty estämään tätä, jos hänen sähköpostinsa on kaapattu.

3. Tunnistautuminen julkishallinnon palveluihin

3.1 Yhtenäinen ratkaisu

Julkishallinnon palveluihin kirjaudutaan nykyään käyttäen suomi.fi -tunnistautumista, mikä tekee kirjautumisen samanlaiseksi kaikissa viranomaispalveluissa. Tämän suomi.fi -sivuston tuottaa Suomen valtiollinen organisaatio Väestörekisterikeskus (VRK) kaiken julkishallinnon puolesta. Sivustosta käytetään myös nimitystä suomi.fi -palveluväylä.

Kun käyttäjä on kirjautunut suomi.fi -palveluun, hän käyttää suoraan kaikkia viranomaispalveluita yhdellä ja samalla kirjautumisella.

Suomi.fi -palvelusivuston muusta sisällöstä on erillinen kuvaus **liitteessä 1**.

Esimerkkejä käytetyimmistä viranomaispalveluista

- Vero
- Omakanta
- Kela
- Trafi (mm. ajoneuvo- ja ajokorttirekisteri)
- Poliisi
- Verkkomaistraatti
- MML (Maanmittauslaitos)
- Terveyskylä; Omapolku

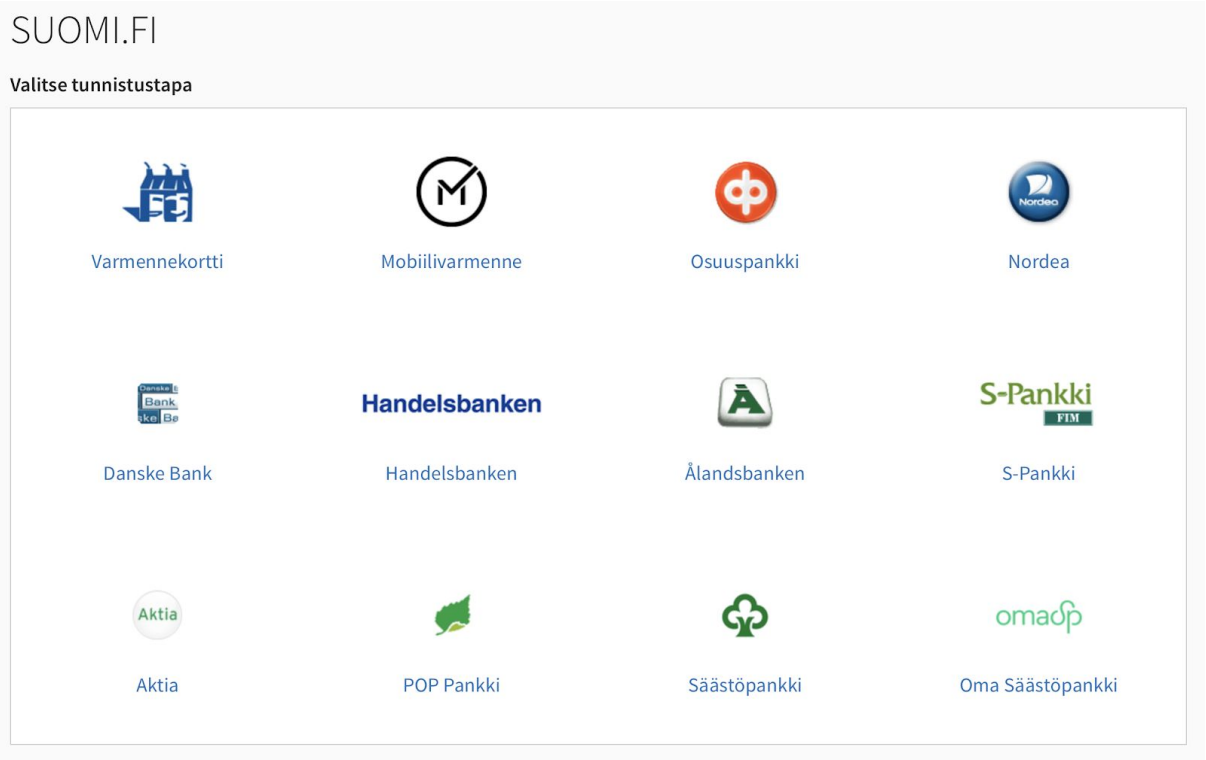
Joissakin kirjautumisissa pyydetään vielä erikseen käyttöehtojen hyväksyntää ja yhteystietojen täydennystä (mm. sähköpostiosoite, puhelin). Kaupungeilla ja kunnilla on suuri joukko omia sähköisiä palveluita. Merkittävässä osassa on jo käytössä suomi.fi -tunnistautuminen.

Suomi.fi -tunnistautumisen ulkopuolella on myös kansalaisille tarkoitettuja palveluja, esimerkiksi:

- Muuttoilmoitus.fi = https://www.posti.fi/muuttoilmoitus
  Yhdellä ilmoituksella Postiin, maistraattiin ja Väestörekisteriin.
  Kirjautuminen tapahtuu pankkitunnuksilla tai henkilökortilla ja myös Postin omilla käyttäjätunnuksilla. Mobiilivarmenne puuttuu tästä ainakin toistaiseksi.
- Kuntien ja kaupunkien kirjastopalvelut perustuvat edelleen kirjastokorttiin ja sen mukaiseen tunnistautumiseen

3.2 Suomi.fi -tunnistautuminen

Kirjautumiselle on kolme perustapaa, jotka esitetään suomi.fi -tunnistautumisen vaihtoehdoissa kuvakelinkkien avulla, kaikki yhdellä sivulla: *varmennekortti*, *mobiilivarmenne* sekä *pankkitunnisteet*. Lisäksi yrityksillä on käytössään ns. katso-tunnistus, joka on Väestörekisterikeskuksen maksuton palvelu organisaatioiden tunnistamiseen sähköisessä asioinnissa. Tähän voi tutustua tarkemmin ”yritys.tunnistus.fi” -sivuilla.



3.2.1 Varmennekortti

Käyttö edellyttää kortinlukijaa, joka liitetään tietokoneeseen USB-liittimellä, erikseen asennettavaa kortinlukuohjelmistoa ja sirullista henkilökorttia. Kortti on poliisin myöntämä henkilökortti, joka on samalla myös passin veroinen tunnistusdokumentti Euroopassa ns. Schengen-alueella.

Varmennekortin käyttöönoton ohjeita joutuu hieman haeskelemaan. Tämän asian ohjeistuksessa kansalaisia varten VRK ei ole onnistunut hyvin. Tietoa aihepiiristä on liikaa, ohjeet ovat osissa siellä täällä ja ylimääräistä vaivaa aiheuttaa se, että organisaatioille tarkoitettu tieto ja ohjeet ovat näillä samoilla sivuilla.

Toivottavasti pian on saatavissa yksinkertainen menettelytapa ja lyhyt ohje, joka koskee vain kansalaisten henkilökortin käyttöönottoa.

Tarkempi esitys varmennekortista ja sen käyttöönotosta on **liitteessä 2**.

3.2.2 Mobiilivarmenne

Tunnistaminen tapahtuu matkapuhelimen avulla. Käyttö edellyttää käyttöönottoa mobiilivarmenne.fi -sivujen kautta. Mobiilivarmenne voi olla maksullinen operaattorin lisäpalvelu.

Mobiilivarmenne on DNA:n, Elisan ja Telian yhteistyön tulos. Sen mainitaan kattavan tällä hetkellä yli 20 000 palvelua eri aloilla (julkiset palvelut, pankki- ja vakuutusasiointi, terveydenhuolto jne.)

Mobiilivarmenne edustaa kaksivaiheista tunnistusta. Koska kirjautuminen pitää vahvistaa fyysisellä laitteella, eli puhelimella, toisen ihmisen henkilöllisyyden väärinkäyttö edellyttäisi myös puhelimen varastamista ja tunnusluvun tietämistä.

Mobiilivarmenteen käyttöönotosta, käytöstä ja palvelun laajuudesta ja on varsin selkeät ohjeet sivuilla mobiilivarmenne.fi.

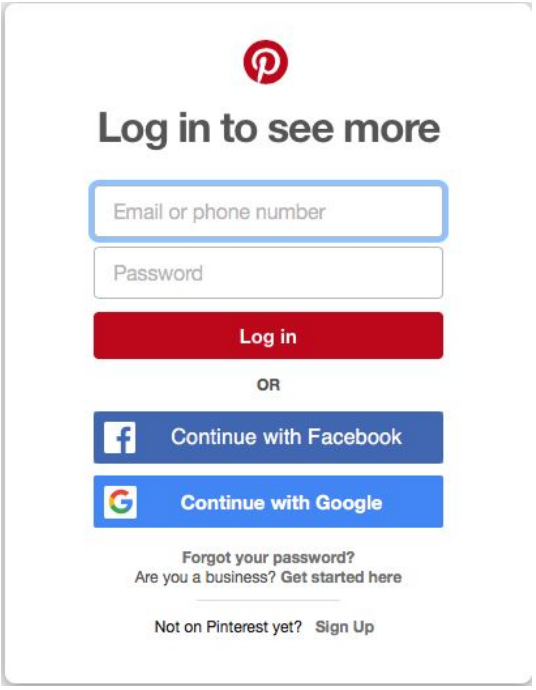
Mobiilivarmenteesta on lisää **liitteessä 3**.

3.2.3 Pankkitunnisteet

Suomi.fi -palveluun on mahdollista kirjautua myös kymmenen eri pankin tunnisteiden avulla. Näitä ei tässä erikseen esitellä, koska pankkien tunnistautumiset poikkeavat hieman toisistaan periaatteen ollessa kuitenkin hyvin samankaltainen. Tässä oletetaan jokaisen osaavan oman pankkinsa tunnistautumismenettelyn.

4. Muita kirjautumistapoja: oikoteitä tai lisäturvaa

4.1 Tunnistautuminen Facebook- tai Google-tunnuksilla

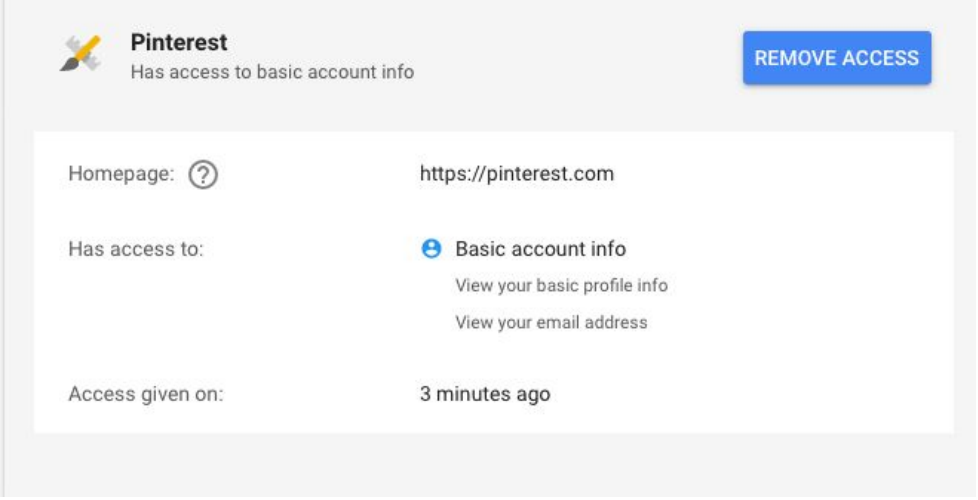


Useat palvelut tarjoavat mahdollisuuden kirjautua Facebook tai Google-tunnuksilla, kuten esimerkiksi Pinterest-sovellus. Käyttämällä Googlen tai Facebookin kirjautumispalvelua ei tarvitse luottaa esim. tässä tapauksessa Pinterestin kykyyn tallentaa käyttäjätietoja turvallisesti, koska palvelu hakee tiedot Googlen tai Facebookin palvelusta.

Useimpien tietoturva-asiantuntijoiden mielestä Googlen palvelun käyttäminen on turvallista ja jopa suositeltavaa, koska tällöin on pienempi riski vaikkapa oman sähköpostin ja muiden tietojen vuotamisesta roskapostittajille. Palvelun tuottaja ei nimittäin saa tallentaa mitään Googlelta hakemiaan tietoja omaan tietokantaansa vaan ainoastaan hakuavaimen.

Periaatteessa Facebook-kirjautuminen toimii samoin kuin Googlen palvelu, mutta ainakaan vielä asiantuntijat eivät luota Facebookin tietojen turvallisuuteen kovinkaan laajasti. Facebook voi myös käyttää hyväkseen tietoa, mihin kaikkiin palveluihin kirjaudut Facebookin kautta. Siten Facebookin käyttämistä kirjautumiseen ei voida suositella.

Googlen palvelusta on myös helppo katsoa, mitä tietoja palveluntuottaja voi Googlen tilitiedoista nähdä ja myös sulkea halutessaan palvelun pääsy tietoihin.



Googlen dokumenteistä löytyvät myös mitä ovat ‘Basic account info’ tiedot:

4.2 Kaksivaiheinen kirjautuminen

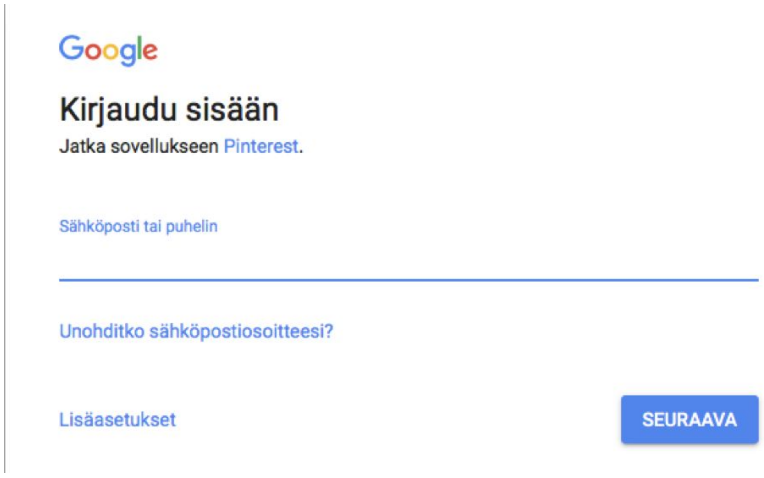
Kaksivaiheinen kirjautuminen lisää turvallisuutta, jos olet tallentanut vaikkapa luottokorttitietoja palveluun. Normaalisti sitä ei kuitenkaan kannata suositella tavalliselle käyttäjälle, koska kaksivaiheisuus hankaloittaa kirjautumista.

Kaksivaiheinen kirjautuminen tarkoittaa käyttäjätunnuksen ja salasanan syöttämisen jälkeen tunnistautumisen vahvistamista toisella laitteella. Tyypillisesti käyttäjä saa esim. tekstiviestin, jossa on 4-6 numeroinen koodi. Koodi pitää sitten syöttää kirjautuakseen palveluun.

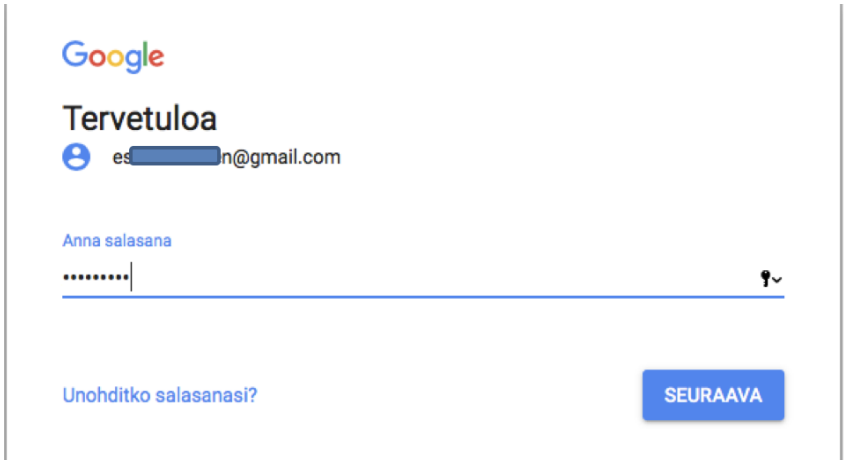
Usein voi hyväksyä laitteen luotetuksi, jolloin kaksivaiheista tunnistautumista ei enää kyseisellä laitteella vaadita. Jotta kaksivaiheisen tunnistautumisen saa päälle, pitää tilin turvallisuusmäärityksissä käydä se ottamassa käyttöön. Sieltä sen saa yleensä myös pois päältä.

Tässä esimerkiksi kirjautuminen Googlen palveluun kaksivaiheisesti.

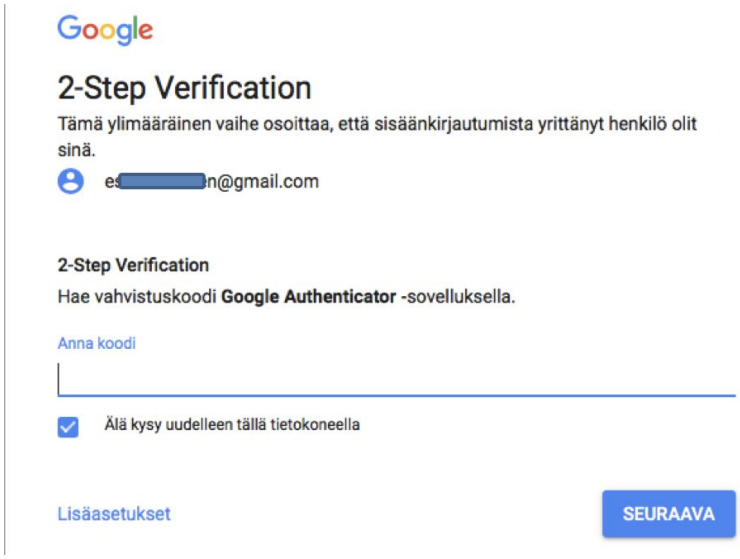
1. Ensin käyttäjätunnus, kuten tavallisessa kirjautumisessa



2. Sitten salasana ihan tavallisesti



3. Sitten vielä koodi, joka lähetetään toiseen laitteeseen, esimerkiksi puhelimeen.



4.3 Sovellussalasanat

Sovellussalasanat liittyvät läheisesti kaksivaiheiseen kirjautumiseen. Sovellussalasanat luodaan kirjautumalla palveluun ja hakemalla tilin hallinnasta oikea toiminto.

Esimerkiksi jos käytät iOS laitteessa Gmailia ja sähköpostiappia sekä kaksivaiheista kirjautumista Googleen, appille pitää luoda oma sovellussalasana Googlen tilin hallinnassa.

5. Mobiililaitteen vaihto

On huomioitava, että sekä mobiililaitteen vaihdossa että täydellisessä tehdasasetusten palauttamisessa joutuu kirjautumaan sisään jokaiseen laitteelle asennettuun palveluun ja antamaan salasanan. Ennen kyseistä toimenpidettä on hyvä listata itselleen kaikkien palveluiden kirjautumistunnukset ja salasanat.

Android laitteella kannattaa ottaa pilvipalveluun varmuuskopio, jotta laitteen tietojen palautus on mahdollista. Se on yleensä laitteen asetuksista määriteltävä Google-tiliin pohjautuva varmuuskopio.

Samsung-laitteille voi luoda myös oman Samsung käyttäjätilin, jolla on mahdollista ottaa oma varmuuskopio laitteesta. Tämä varmuuskopio on täydellisempi kuin esim. Google-tilin ottama kopio. Se sisältää esim. enemmän tietoa käyttäjän laitteen näytöille tekemistä muokkauksista. Toimii palautettaessa varmuuskopio joko uuteen tai huollettuun Samsung laitteeseen.

Applen iCloud-varmuuskopiosta voi myös palauttaa vanhan laitteen tiedot uuteen Apple-laitteeseen.

6. Kirjautumisilmoitukset ja varoitukset

6.1. Ilmoitusten tarkoitus

Eri palveluihin kirjautumisen yhteydessä käyttäjä voi saada ao. palvelun tarjoajalta erilaisia ilmoituksia. Ilmoitus voi tulla samalla hetkellä näytölle tai tyypillisesti myös sähköpostiin tai tekstiviestinä puhelinnumeroon, jotka on annettu alun perin yhteystiedoksi ao. palvelun käyttäjätunnuksia luotaessa.

Näiden ilmoitusten tärkein tarkoitus on tietosuoja, jolloin kontrolloidaan poikkeuksia ja muutoksia ao. järjestelmään kirjautumisissa. Tyypillisesti uudella laitteella, oudosta sijainnista tai toisinaan jopa uudella selaimella kirjautuminen aiheuttaa tällaisen ilmoituksen ja myös henkilöllisyyden varmistuskyselyn.

Näitä ilmoituksia ei tarvitse millään tavalla ”säikähtää”, vaan kysymys on käyttäjän hyödystä ja turvallisuudesta. Näissä viesteissä ehdotetut toimenpiteet ja tarkistukset kannattaa aina tehdä loppuun saakka, jotta ao. käyttäjätilien turvallisuuteen liittyvät tiedot pysyvät kunnossa. Viestien alkuperä on myös hyvä tarkistaa (lähettäjätiedot tms.), koska hämäysviestejä ja tietojen kalastelijoita on verkossa liikkeellä.

6.2. Esimerkkitapaukset

Eri palvelujen tarjoajilla on kullakin omat ilmoitukset ja menettelytavat. Keskinäisiä eroavuuksia ilmenee myös tietokoneille, tableteille ja puhelimille tulevilla ilmoituksilla. Erilaisten ilmoitusten ja varoitusten määrä on siten huomattavan suuri, joten seuraavassa esitellään vain joitakin tärkeitä esimerkkejä.

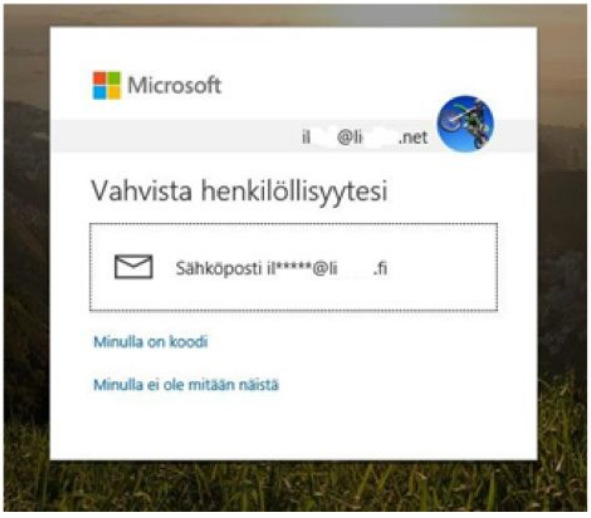
Ilmoitusten muoto ja sisältö luonnollisesti muuttuvat ajan kuluessa ja uusien ohjelmistoversioiden myötä. Siksi kannattaa kiinnittää erityistä huomiota tarkoitukseen ja tarvittaviin toimintatapoihin kussakin tilanteessa. Ne ovat pysyvämpiä kuin ilmoitusten tarkka ulkoasu. Mukaan esimerkkeihin on valittu Microsoftin, Googlen, Facebookin ja Applen kirjautumisilmoituksia. Vaikka ilmoitukset suomenkielisiin sovelluksiin tulevat pääsääntöisesti suomeksi, ovat englanninkieliset ilmoitukset myös tavallisia.

Joissakin esimerkeissä jäljempänä viitataan käyttäjätilin asetuksista löytyviin toimintoihin. Kannattaa muistaa, että esim. Googlen ja Facebookin täysikokoinen selainkäyttö tietokoneella näyttää monet tarvittavat ilmoitus- ja turva-asetukset paremmin, kuin mihin mobiililaitteiden vastaavat sovellukset pystyvät.

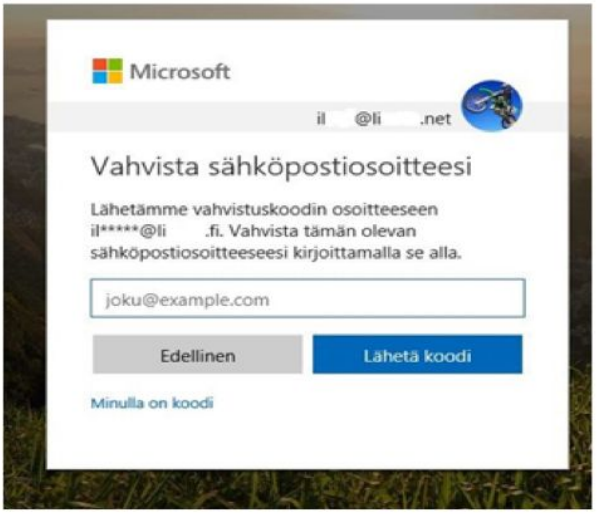
6.2.1 Microsoft

Microsoft-tili tarvitaan, jos käytössä on jokin Microsoftin palveluista (Outlook.com, Office365, Skype, OneDrive jne.). Kirjautumisen poikkeustilanteissa myös Microsoft tarvitsee käyttäjiltään henkilöllisyyden vahvistamisen. Tavanomainen vahvistamiskäytäntö, missä Microsoft lähettää käyttäjätilille ilmoitettuun sähköpostiosoitteeseen vahvistuskoodin, on vaiheittain esitetty seuraavassa:

Vaihe 1:



Vaihe 2:



Vaihe 3:

Microsoft account

Security code

Please use the following security code for the Microsoft account il*****@lixxxxx.net.

Security code: **7119799**

If you don't recognize the Microsoft account il*****@lixxxx.net, you can click here to remove your email address from that account.

Thanks,
The Microsoft account team

Vaiheessa 3 tullutta vahvistuskoodia (security code) kysytään sitten erikseen seuraavan kirjautumisen yhteydessä.

Microsoft on ohjeistanut tilin käyttöä koskevat säännöt ja käytännöt varsin seikkaperäisesti. Ohjeet löytyvät seuraavan linkin takaa: https://support.microsoft.com/fi-fi/products/microsoft-account?category=sign-in-issues

6.2.2. Google

Gmailin, Google Driven tai Android-laitteen jne. käyttäjillä on Google-tili. Usein samaa tiliä käytetään kerralla monella laitteella: tabletti, matkapuhelin ja tietokone. Lisäksi niissä voidaan olla samaan aikaan kirjautuneena.

Kirjauduttaessa Google-tilille, siis myös johonkin Googlen palveluun, on joskus suoritettava ylimääräinen vaihe henkilöllisyyden vahvistamiseksi. Tämä tehdään ainakin silloin, kun Google havaitsee jotain epätavallista kirjautumistavassa, esim. uusi laite tai normaalista poikkeava sijainti.

- kirjaudu sisään tavalliseen tapaan.
- jos näet henkilöllisyyden vahvistusnäytön, suorita tehtävä tai valitse ”kokeile toista sisäänkirjautumistapaa”
- käytettävissäsi on osa tai kaikki näistä vaihtoehdoista:
    - saat kehotteen puhelimeen.
    - saat vahvistuskoodin tekstiviestillä.
    - saat vahvistuskoodin puhelimitse.
    - saat vahvistuskoodin Android-laitteeseesi.
    - vastaa turvakysymykseen.

Tämä ylimääräinen vaihe suojaa käyttäjätilin siltä varalta, että joku muu yrittää kirjautua sisään. Vaikka joku saisi selville käyttäjänimen ja salasanan tietojenkalastelulla tai muuta kautta, hän ei voi kirjautua sisään ilman Googlelle ilmoitettua puhelinta.

Välillä voi olla hyvä tarkistaa, mitä kaikkia laitteita tilille on kytketty, ts. millä laitteilla Googlen palveluja on käytetty oman tilin kautta. Google-tilin tiedoista löytyy ”laite- ja tietoturvatapahtumat”, jonka avulla näkee, mitkä laitteet on kytketty Google-tiliin ja mistä

käsin niitä käytetään. Jotta omia tietoja pääsee katsomaan, täytyy kirjautua sisään Google-tunnuksilla.

Näkymässä voi poistaa tililtä laitteet, jotka eivät ole enää käytössä. Samoin kannattaa tehdä tuntemattomille laitteille. Mikäli näitä ilmenee, näkymä kertoo myös, mistä käsin laitteita käytetään. **Tällaisessa tilanteessa laitteen poistamisen ohella kannattaa vaihtaa Google-tunnuksen salasana.**

Googlen-tilin hallinnointiin on tarjolla seikkaperäinen ohjeistus ohjekeskuksessa, jonka osoite on seuraava: https://support.google.com/accounts#topic=3382296

Ohjeistus on selkeä, mutta laaja. Useimmat kirjautumis- ja salasanaongelmat selviävät tämän avulla, joten Google-käyttäjien kannattaa tutustua sen sisältöön. Monelle kysymykselle ja käytön sekaannukselle voi löytyä helppo selitys ja ratkaisu, myös opastustilanteissa.

Uudella laitteella kirjautuminen voi aiheuttaa myös seuraavan ilmoituksen sähköpostiin:

Google

Ilkka xxxxx

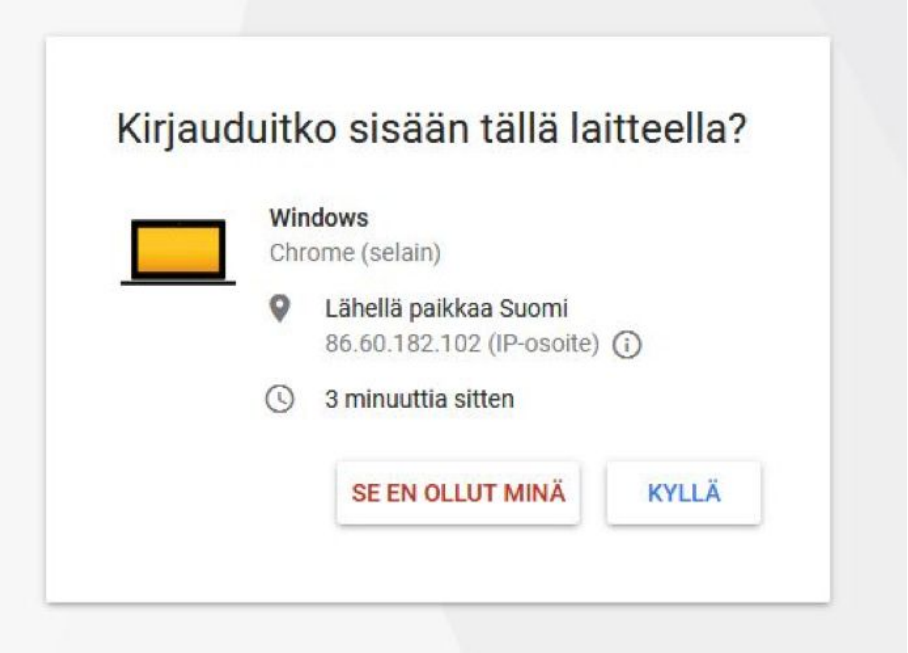
Kirjautuminen uudelta laitteelta tilille
ilkka@xxxxx.net

TARKISTA TOIMINTA

Google-tililläsi kirjauduttiin juuri uudella laitteella (Windows). Lähetimme tämän sähköpostin varmistaaksemme, että sinä teit sen.

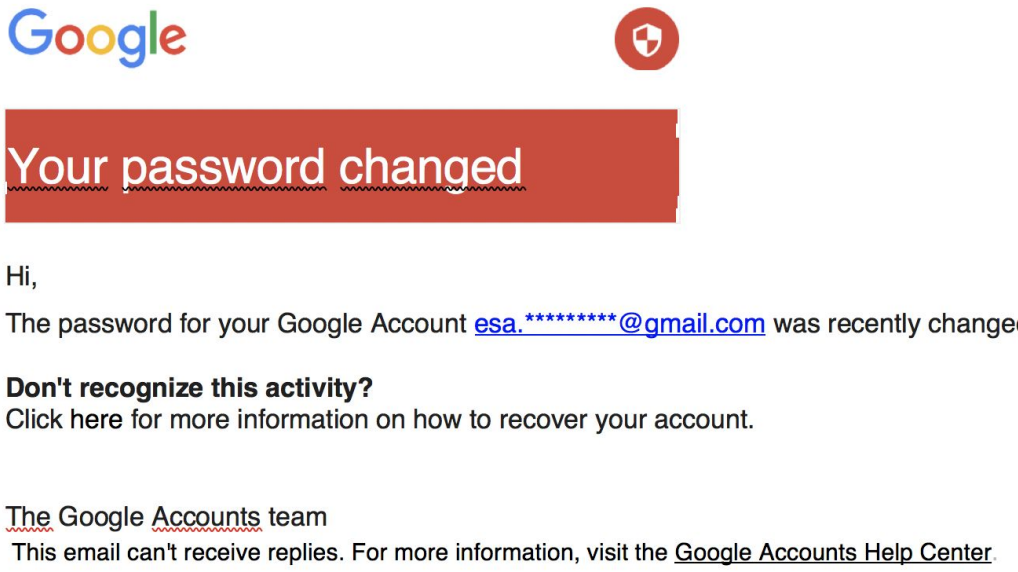
Kerromme tällä sähköpostilla tärkeistä Google-tilin ja -palveluiden muutoksista.
© 2018 Google Inc.,1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Tämän ilmoituksen mukaisesti on tarpeellista vahvistaa henkilöllisyys “tarkista toiminta” -painikkeen kautta. Seuraavaksi tulee kysymys, jossa mainitaan ao. laitteesta joitain tunnistamistietoja (käyttöjärjestelmä, selain jne). Paikkaakin ehdotetaan, mutta tieto voi olla myös väärin tai liian epämääräinen johtuen esim. verkko-operaattorien mobiiliverkkojen sisäisistä järjestelyistä.



Jos tämä on oma kirjautuminen, valitsemalla “kyllä” tulee vahvistus henkilöllisyydestä. Jos tätä kirjautumista ei ole itse tehty, on mahdollista, että Googlen käyttäjätunnus on joutunut vääriin käsiin. Vaihda sen salasana mahdollisimman pian.

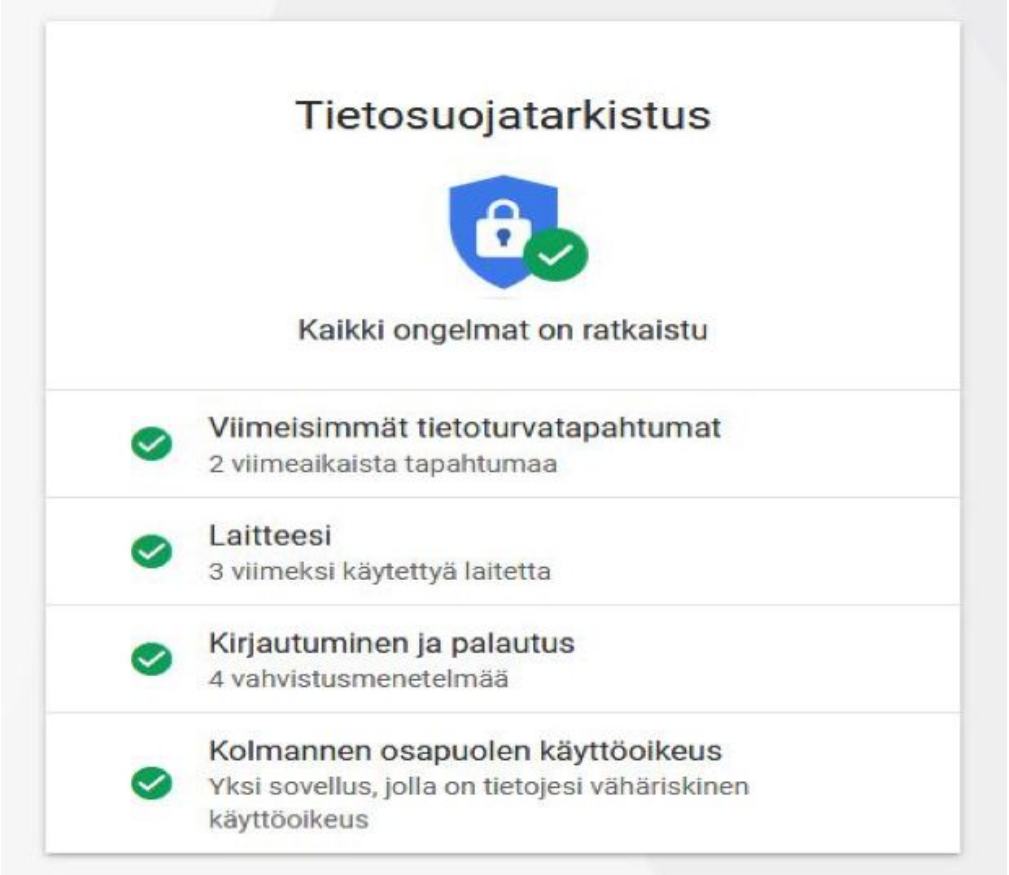
Salasanan vaihto aiheuttaa Googlen seuraavan ilmoituksen.



Ilmoitus on toteamus tapahtuneesta. Jos sitä ei ole itse tehty, asialla on sitten joku vieras henkilö, joka on näin saanut tilin haltuunsa. On vielä mahdollisuus palauttaa tili takaisin omaan käyttöösi (recover). Tällöin toimitaan siis samalla tavalla, kuin salasana olisi unohtunut.

Uudella mobiililaitteella kirjautuminen (esim. läppäri tai tablet) johonkin Googlen palveluun voi aiheuttaa myös tunnistamisen puhelimen avulla, jos Googlella on tiedossa puhelinnumerosi. Google lähettää puhelimeen kertakäyttöisen numerokoodin, joka pitää vahvistaa uuden laitteen kirjautumisnäytöllä.

Googlen tietosuojatarkistus on toiminto, joka löytyy myös Googlen ”oma tili” -kirjautumisen takaa. Sen avulla pystyy tarkistamaan käytettyjä laitteita ja kirjautumisia.



6.2.3. Facebook

Facebookiin kirjautuminen tarvitsee muiden palvelujen lailla käyttäjätunnuksen ja salasanan. Tärkeää on muistaa, että jos Facebookista ei kirjauduta ulos, istunto (yhteys) jää päälle. Tämä tarkoittaa sitä, että seuraava tietokoneen käyttäjä pääsee suoraan tilille, kun hän avaa Facebookin. Facebookin käyttäminen selaimella jollakin muulla kuin omalla tietokoneella muodostuu näin selväksi riskiksi unohtamisen takia.

Facebookissa voi tarkastella, moneltako koneelta on aktiivinen istunto menossa tai miltä laitteilta on kirjauduttu. Nämä näkee parhaiten Facebookin täyskokoisella selainversiolla.

Asetuksiin pääsee klikkaamalla yläpalkissa oikealla olevaa hammasrattaan tai kolmiomaisen nuolen kuvaa. Tämän takaa aukeavasta valikosta valitaan ”Asetukset” ja vasemmalle aukeavasta valikosta ”Turvallisuus ja sisäänkirjautuminen”. Täällä näkyvät listana viimeaikaiset kirjautumiset ja myös avoimet istunnot, mukaanlukien tabletit ja älypuhelimet.

Istunnot pystyy lopettamaan klikkaamalla ao. laitteen kohdalla ”Kirjaudu ulos” -valintaa. Sen jälkeen Facebook pyytää salasanaa seuraavan kerran kyseiseltä laitteelta kirjauduttaessa, paitsi jos salasana on tallennettu selaimen omalla ”Tallenna salasana” -toiminnolla.

Facebook-tiliin kirjautumisen turvallisuutta voi lisätä, jos ottaa käyttöön ilmoitukset, kun uudelta laitteelta kirjaudutaan tilillesi ensimmäistä kertaa. Ilmoituksen voi valita tulemaan sähköpostitse tai tekstiviestitse. Jälkimmäinen edellyttää puhelinnumeron antamista Facebookille. Tätä varten Facebookin tiliasetuksista löytyy valinta (kohdassa ”Turvallisuus ja sisäänkirjautuminen”):

Sähköpostitse tuleva ilmoitus on seuraavan kaltainen:

6.2.4. Apple

Apple pitää kirjaa myös kaikista Apple ID -tilillä käytetyistä laitteista. Useimmat edellä mainitut tilanteet on huomioitu myös Applen ilmoituksissa ja varoituksissa. Seuraavassa on esimerkkiviesti tilanteesta, missä Apple-tilille on lisätty uusi laite:

Hyvä Esa ********

Seuraavat Apple ID:si e·····@********.com tiedot päivitettiin 15. marraskuuta 2017.

Luotettu laite lisätty - iPhone Xyx

Luotettuja laitteitasi käytetään vahvistamaan henkilöllisyytesi, kun teet muutoksia tiliisi, kirjaudut iCloudiin tai teet iTunes Store- tai App Store -ostoja uudelta laitteelta.

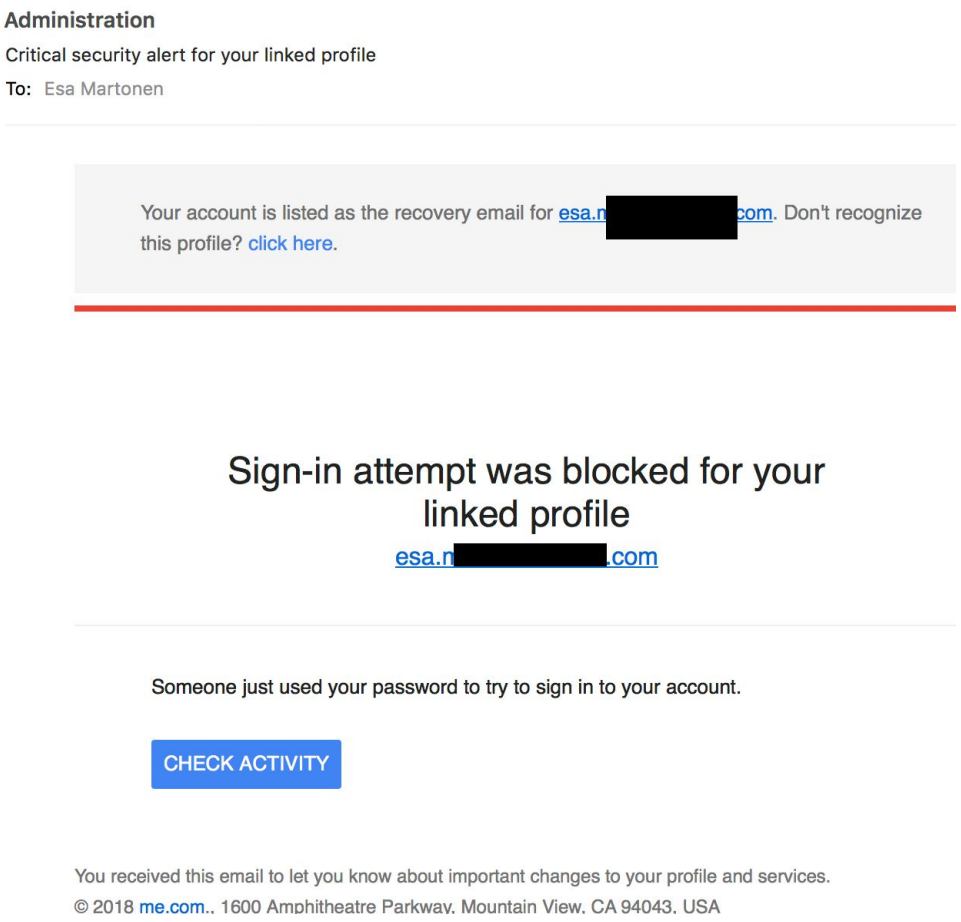
Turvallisuutesi takaamiseksi luotettu laite poistetaan tililtäsi, jos se tyhjennetään tai jos jostain syystä emme voi enää luottaa siihen. Voit vahvistaa laitteesi uudelleen tai lisätä uuden laitteen kohdassa Turvallisuus Apple ID -sivustollasi

Ystävällisin terveisin

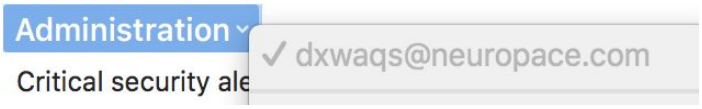
Apple-tuki

6.3. Huijaukset

Rikolliset osaavat käyttää myös varoitusviestejä omiin tarkoituksiinsa tekemällä ne tarkoin muistuttamaan tarkoin oikeita viestejä. Esimerkiksi seuraava sähköposti näyttää aidolta:



Mutta kun katsot lähettäjää tarkemmin voit nähdä todellisen lähettäjän osoitteen:



Viesteistä tulee aina tarkistaa todellinen lähettäjän osoite. Lisäksi pitää välttää viesteissä olevien linkkien ja painikkeiden painallusta, ellei todellista nettiosoitetta pysty varmistamaan.

Liite 1: Suomi.fi -sisällöstä tarkemmin

Suomi.fi -palvelun avulla pystyy käyttämään seuraavia informaatio- yms. palveluita:

- Viranomaisviestit ja -päätökset sähköisesti (”suomi.fi -postilaatikko”). Postilaatikkoon pystyy asettamaan ilmoitusviestin lähettämisen omaan päivittäisessä käytössä olevaan sähköpostiin. Viesti on vain ilmoitus tulleesta viestistä, joka pitää käydä lukemassa suomi.fi -palvelun kautta.
- Palvelussa voi tehdä myös valtuutuksia omasta puolesta tai pyytää niitä toiselta, joka vahvistaa pyynnön oman suomi.fi -kirjautumisen jälkeen ao. kohdassa. Suomi.fi-valtuuksissa voi valtuuttaa toisia henkilöitä tai yrityksiä toimimaan puolesta valituissa asioissa ja voi pyytää valtuutta asioida toisen henkilön tai yrityksen puolesta. Palvelun listausnäkymien avulla hallinnoidaan annettuja ja saatuja valtuuksia sekä valtuuspyyntöjä. Esim. läheisen ihmisen puolesta omakanta-asiointia tai lääkereseptien uusimista voi näin sujuvoittaa.
- Suomi.fi voit tarkistaa myös suoraan ja nopeasti, mitä rekisteritietoja itsestä löytyy mm. seuraavista paikoista:

    VRK Väestörekisteri

    Trafi Ajoneuvot, ajokorttitiedot, vesikuluneuvot

    MML Maanmittauslaitos

    PRH Patentti- ja rekisterihallitus, kaupparekisteri

    Kansalaisaloite

    Kuntalaisaloite

Suomi.fi -kehitystyö jatkuu. Siten sen sisältöön tulee lisäyksiä ja muutoksia ajan kuluessa. Se ei korvaa eri viranomaisten omia nettipalveluja, jotka ovat toteutettu ao. hallinnonalan omia tarpeita varten. Tällä hetkellä näyttää siltä, että sinne on tarkoitus koota nimenomaan informaatiota ja sellaisia yhteisiä toimintoja, jotka eivät ole minkään yksittäisen viraston vastuulla.

Liite 2: Varmennekortista tarkemmin

Varmennekortin käyttöönotto

Henkilökortin lisäksi kansalaisvarmenteen käyttöön tarvitaan tietokone, kortinlukija ja kortinlukijaohjelmisto.

Ohjeita ei löydy suomi.fi -sivuilta vaan asiat löytyvät sivulta http://vrk.fi/palvelut-kansalaisille, missä on kohta ”Kansalaisvarmenne ja sähköinen henkilöllisyys” ja sen alla linkki ”Kansalaisvarmenteen käyttöönotto”. Sen jälkeen ohjelmiston latauslinkki löytyy tekstin seasta kohdassa ”Kansalaisvarmenteen käyttöönotto ja käyttö”.

Linkki johtaa VRK:n Eevertti-palveluun. Tämän kirjoittamisen hetkellä (15.3.2018) jakelussa oleva mPollux Digisign Client -ohjelmisto on saatavilla Windows 7:aan ja uudemmille versioille, parille Linux-versiolle ja MacOS:lle (10.9 - 10.13). Kortinlukijaohjelmisto sisältyy varmennekortin hintaan, ja sen voi ladata maksutta.

Lataukseen on valinnaisesti ”paketoitu” mukaan myös Fujitech- kortinlukijan ohjaimien lataus. Kortinlukijaa myy Verkkokauppa.com hintaa vähän yli 20 euroa. Muutkin ao. ISO-standardin mukaiset kortinlukijat ovat toimivia. Jokin ei-ilmoitettu syy on johtanut VRK:n jakelemaan tätä Fujitechin ohjainta.

1.1.2017 jälkeen

1.1.2017 jälkeen haetut henkilökortit tarvitsevat käytön aloituksessa aktivointitunnuslukua. Aktivointitunnusluku toimitetaan postitse viikon kuluessa kortin toimittamisesta.

Kortinlukijaohjelmisto käynnistää aktivointiprosessin automaattisesti, kun henkilökorttia käytetään ensimmäisen kerran. Aluksi käyttäjältä kysytään aktivointitunnusluku ja tämän jälkeen käyttäjä määrittää omat henkilökohtaiset PIN-tunnuslukunsa. Toinen on perustunnusluku ja toista tarvitaan sähköiseen allekirjoitukseen. Mikäli käyttäjä antaa aktivointitunnusluvun viisi kertaa väärin, kortti lukittuu pysyvästi.

Ennen 1.1.2017

Ennen 1.1.2017 haetuille kortteille on oheispostituksena tullut kirje, jossa ovat henkilökohtaiset tunnusluvut, PIN1 ja PIN2, annettuna valmiina. Käyttöönottoon käyvät samat ohjelmistot kuin uudempiin kortteihin. Käyttö aloitetaan antamalla onnistuneen asennuksen jälkeen PIN1-luku tunnistautumisessa.

Windows-ohjelmiston lataus ja asennus

Yksittäiseen koneeseen tarvitaan uusin DigiSignClient 4.0.14 -versio (yhteinen exe -paketti). Windows 7:ää vanhempia versioita ei tueta.

Latauksessa ohjelmisto menee Lataukset-kansioon (Downloads), josta sen voi asentaa yksinkertaisesti vain käynnistämällä (Run). Asennus kysyy kielen, muuten oletusarvot ovat ok. Jos käytössä on Fujitechin kortinlukija, tässä kohtaa voi valita myös sen ohjaimien asennuksen.

Varmennekortin käyttö

Aluksi kortinlukijan pitää olla liitettynä tietokoneeseen. Valitaan Varmennekortti-kuvake suomi.fi -tunnistautumisessa ja seurataan ruudulle tulevia ohjeita. Kun seuraavaksi laitetaan kortti lukijaan, pitää odottaa luku loppuun joitakin sekunteja - lukijassa on merkkivalo tähän. Sen jälkeen vain painetaan tunnistaudu-painiketta.

Seuraavaksi kysytään sertifikaatin hyväksymistä, ao. ruutu on eri selaimilla hieman erilainen (Confirm certificate). Tämän jälkeen, jos kaikki vaiheet menevät onnistuneesti läpi, kirjautuminen avaa ao. palvelun, mihin oltiin menossa.

Jokainen tunnistautuminen vaatii kortin lukua, joten korttia ei voi jättää lukijaan pysyvästi, vaan vain kulloisenkin käytön ajaksi.

Virhetilanteista:

Kaikki selaimet eivät heti toimi. Mm. Firefox voi vaatia lisäasetuksia. Ohjeita saa Digisign-ohjelmiston oppaasta. (https://eevertti.vrk.fi/documents/2634109/2853195/DigiSign+asennus-+ja+k%C3%A4ytt%C3%B6ohje.pdf/852eea48-8207-4d7d-8a72-c3b9ec227833)

Jos selain menee heti ensimmäisellä kerralla virheeseen, nopein tie eteenpäin on jonkin toisen selaimen kokeilu. Sellaisillakin selaimilla, joilla edellisellä kerralla kaikki meni ok, tunnistautuminen voi mennä virheeseen. Silloin selaushistorian eli välimuistin tyhjentäminen ennen uutta yritystä useimmiten auttaa. Järjestelmä ei sitä aina erikseen ehdotakaan.

Liite 3: Mobiilivarmenteesta tarkemmin

Mobiilivarmenteen käyttöönotto:

- mene sivulle mobiilivarmenne.fi
- valitse oma matkapuhelinoperaattorisi (DNA, Elisa, Telia) ja
  -> siirry palveluun
- anna puhelinumero
- paina nappia ”lähetä salasana”
- salasana tulee tekstiviestillä
- täytä se kenttään ja lähetä
- sen jälkeen vahvistetaan henkilöllisyys pankkitunnuksilla

Mobiilivarmenteessa ovat mukana OP, Danske Bank, S-Pankki, Aktia, Handelsbanken, OmaSP ja POP_Pankki, Nordea ei ole tällä hetkellä mukana tässä listassa.

Järjestelmä näyttää myös operaattorilla olevat yhteystiedot ja pyytää tarkistamaan ne. Sen jälkeen järjestelmä pyytää antamaan kaksi itse valittua tunnuslukua

- (perus)tunnusluku (4-8 numeroa)
- allekirjoitustunnusluku (6-8 numeroa)

Kirjoita tunnusluvut muistiin!!

Lopuksi tulee vahvistus, jossa on mainittu sähköinen asiointitunnus (sama kuin varmennekortissa, jos sellainen on käytössä). Vähän ajan kuluttua tulee vielä tekstiviesti-ilmoitus, joka vahvistaa palvelun olevan käytettävissä.

Varmenteen voimassaoloaika on 5 vuotta. Palvelun voi halutessa lopettaa milloin vain.

Yksityishenkilöiden hinnat Elisalla ja DNA:lla ovat ensimmäinen 12 kk 0 euroa ja sen jälkeen 1,99 / kk (vuoden 2018 hinnaston mukaan). Telian hinnastossa palvelu on maksuton.

Mobiilivarmenteen käyttö

Jos tunnistautumisessa on vaihtoehtona mobiilivarmenne, käyttäminen on ilahduttavan yksinkertaista:

- kirjautumisessa annetaan puhelinnumero, jolla mobiilivarmenne on rekisteröity
- puhelimen näyttöön tulee välittömästi ilmoitus, johon annetaan (perus)tunnusluku
- hetken päästä yhteys haluttuun palveluun aukeaa tietokoneella automaattisesti

Mobiilivarmenteen käytössä voi tulla myös virhetilanne, jolloin järjestelmä antaa seuraavan virheilmoituksen:

> *Tunnistautumisessa tapahtui virhe ja tunnistautuminen keskeytyi. Tietosi eivät kuitenkaan ole vaarantuneet, eivätkä ne voi päätyä vahingossa muiden tietoon.*
>
> *Ratkaistaksesi tilanne kokeile seuraavia toimia:*
>
> - *Tyhjennä selaimen välimuisti ja tunnistaudu sen jälkeen uudelleen*
> - *Tunnistaudu uudelleen käyttämällä toista selainta*

Siis jos ko. selain on jo aiemmin toiminut hyvin, selaimen välimuistin (historiatiedot) tyhjentäminen auttaa useimmiten.