

Aleksi Tamminiemi

# MONIVAIHEINEN TUNNISTAUTUMI- NEN

Opinnäytetyö

Tekniikan ammattikorkeakoulututkinto

Tieto- ja viestintätekniikan koulutus

2021



**Kaakkois-Suomen  
ammattikorkeakoulu**

Tutkintonimike	Insinööri (AMK)
Tekijä	Alexi Tamminiemi
Työn nimi	Monivaiheinen tunnistautumisen
Toimeksiantaja	Kaakkois-Suomen Ammattikorkeakoulu Oy
Vuosi	Toukokuu 2021
Sivut	40 sivua, joista liitteitä 1 sivu
Työn ohjaaja(t)	Marko Oras

## TIIVISTELMÄ

Monivaiheinen tunnistautuminen on jo monelle tuttua työelämästä. Tästä huolimatta kaikki eivät ole omaksuneet sitä osaksi yksityistä tietoturvaansa. Kaikille käyttäjäryhmille monivaiheisen tunnistautumisen hyödyt eivät ole selviä, ja sen käyttöönotto koetaan hankalaksi. Yksityishenkilön käytössä olevien palveluiden määrän kasvaessa kasvaa myös tunnistautumisten määrä. Useiden eri tunnuksien muistaminen ei ole käyttäjäystävällistä ja siksi useat käyttävät vastoin suosituksia samaa salasanaa useissa eri palveluissa.

Tämän opinnäytetyön tavoitteena oli madaltaa monivaiheisen tunnistautumisen käyttöönottoa yksityishenkilön näkökulmasta sekä tuoda esille sen tarjoamia hyötyjä. Työssä käsitellään erilaiset tunnistetyypit, niiden vaatimukset ja hyödyt. Tämän lisäksi käydään lävitse yleisimmät monivaiheisen tunnistautumisen menetelmät ja näiden käyttöönotosta esitellään yksityiskohtainen kirjattu ohjeistus.

Tutkimuksen edetessä koettiin hyödylliseksi lisätä osio salasanan hallintaohjelmista näiden ollessa osa yksityishenkilön tietoturvaa. Näistä tutkittiin kahta niiden ominaisuuksien perusteella valikoitua hallintaohjelmaa. Työssä käytiin läpi kummankin hallintaohjelman turvallisuus, käyttöönotto ja käyttö. Tämä lisäksi tutkittiin yleisesti salasanan hallintaohjelmiin kohdistuvia riskejä.

Tutkimus toteutettiin laadullisella tutkimusmenetelmällä. Työssä analysoitiin asiantuntijakirjoituksia sekä teknologiayrityksien tuottamaa dokumentaatiota johtopäätöksiä tekemiseen.

Monivaiheinen tunnistautuminen tulee olemaan tulevaisuudessa lähes välttämätön. Sen tarjoamat hyödyt tietoturvalle ovat kiistämättömiä. Työlle asetettuihin tavoitteisiin päästiin tuottamalla helposti luettava ja ymmärrettävä opastus monivaiheisen tunnistautumisen menetelmistä, niiden hyödyistä ja käyttöönotosta. Tämän perusteella käyttäjät voivat tehdä päätöksen heidän tilanteeseensa sopivasta tunnistautumismenetelmästä.

Teknologian kehittyessä, tarjoaa se uusia tunnistetyyppejä, parantaa jo olemassa olevia tai tulee yhdistämään näitä toisiinsa.

**Asiasanat:** todentaminen, tunnisteet, tietoturva

Degree	Bachelor of Engineering
Author	Aleksi Tamminiemi
Thesis title	Multi-factor authentication
Commissioned by	Kaakkois-Suomen Ammattikorkeakoulu Oy
Time	May 2021
Pages	40 pages, 1 page of appendix
Supervisor	Marko Oras

## ABSTRACT

Multi-factor authentication is already familiar to many as a part of their job. Despite this, not everyone has taken it as a part of their information security. For some user groups the benefits of multi-factor authentication are not clear, and its implementation is perceived as cumbersome. As the number of services per individual user increases, so does the number of required authentications. It is not perceived as user-friendly for a person to remember several different passwords and therefore many people still use the same password in different services, contrary to the recommendations.

The objective of this thesis was to lower the introduction of multi-factor authentication from the perspective of an individual, and to highlight the benefits it offers. This thesis reviewed different types of identifiers, their benefits and requirements. In addition, the most common multi-factor authentication methods were reviewed and detailed instructions were recorded for their implementation.

As the thesis progressed, it was found useful to add a section on password managers as they are an important part of personal information security. Two password managers were selected based on their features. The security of both password managers was reviewed. Additionally, instructions on their use and implementation were recorded. Possible risks regarding password managers were researched and documented.

The research was carried out using a qualitative research method. This thesis analyzed expert writings, as well as documentation produced by technology companies to draw its conclusions.

In the future multi-factor authentication will be a more essential part of information security. The benefits offered by multi-factor authentication are undeniable. The goals set for this thesis were met by producing easy to read and easy to understand documentation on multi-factor authentication methods, their benefits and how to implement them. Based on this, users can make an educated decision on what multi-factor authentication method is appropriate for their situation.

As technology keeps advancing, it will offer new types of identification methods, enhance existing ones, or combine these.

**Keywords:** authentication, identifiers, information security

## SISÄLLYS

1	JOHDANTO .....	7
2	TUTKIMUKSEN TOTEUTUS .....	8
2.1	Tutkimusongelma ja -kysymys .....	9
2.2	Tutkimusmenetelmä .....	9
3	MONIVAIHEINEN TUNNISTAUTUMINEN .....	10
3.1	Tunnistetyypit .....	11
3.2	Jotain mitä tiedät .....	11
3.3	Jotain mitä omistat .....	12
3.4	Missä olet .....	12
3.5	Jotain mitä olet .....	12
4	MOBIILIVARMENNE .....	13
4.1	Käyttöönotto .....	13
4.2	DNA .....	14
4.3	Elisa .....	16
4.4	Telia .....	18
4.5	Käyttö .....	19
4.6	Mobiilivarmenteen tekniset tiedot .....	20
5	GOOGLE .....	20
5.1	Käyttöönotto .....	21
5.2	Käyttö .....	22
6	MICROSOFT .....	23
6.1	Käyttöönotto .....	24
6.2	Käyttö .....	25
7	SALASANAN HALLINTAOHJELMISTOT .....	25
7.1	KeePass .....	26
7.1.1	Turvallisuus .....	26

7.1.2 Käyttö .....	27
7.2 F-Secure ID PROTECTION .....	28
7.2.1 Turvallisuus .....	29
7.2.2 Käyttö .....	30
7.3 Riskit .....	33
8 YHTEENVETO .....	33
8.1 Pohdinta .....	34
8.2 Jatkokehitys .....	35
LÄHTEET .....	36
KUVALUETTELO	
LIITTEET	

Liite 1. Infograafi Monivaiheinen tunnistautuminen

## KÄSITTEET

AES-256	Advanced Encryption Standard (AES). AES-256 on 256 bittiä pitkää avainta käyttävä salausalgoritmi.
Bluetooth	Lyhyen kantaman langaton tiedonsiirtotekniikka
Tiivistefunktio	Funktio, jolla datalle voidaan laskea määräpituinen hajautusarvo
HMAC	Hash-based message authentication code (HMAC). Hajautusarvoon perustuva viestin todennuskoodi
ICCID	Integrated circuit card identifier (ICCID). SIM-kortin yksilöivä sarjanumero
IETF	Internet Engineering Task Force (IETF). Voittoon tavoittelematon avoimia standardeja ylläpitävä organisaatio
Julkisen avaimen menetelmä	Salausmenetelmä, jossa julkista avainta käytetään tietojen salaamiseen
NCSC	National Cyber Security Centre (NCSC). Yhdistyneiden kuningaskuntien kyberturvallisuus viranomainen
NFC	Near-Field communication (NFC). Joukko laitteiden välisiä tiedonsiirtoprotokollia alle 4 cm matkoille
NSA	National Security Agency (NSA). Yhdysvaltojen kansallinen turvallisuusvirasto
PBKDF2	Password-Based Key Derivation Function 2 (PBKDF2). Näennäissatunnainen tiivistefunktio, jolla salasanoja suojataan väsytyshyökkäyksiä vastaan
RSA	Rivest-Shamir-Adleman (RSA) on nimetty suunnittelijoidensa mukaan. Julkisen avaimen menetelmää hyödyntävä salausalgoritmi
SHA-256	Secure Hash Algorithm (SHA). Tiivistefunktio, joka tuottaa 256 bitin hajautusarvoja
Standardi	Asettaa yhtenevät kriteerit

Twofish	Salausalgoritmi, joka käyttää samaa salausavainta salaukseen ja salauksen purkuun.
U2F	Universal 2 <sup>nd</sup> Factor (U2F). Avoin standardi kaksivaiheisen tunnistautumisen yksinkertaistamiseen ja vahvistamiseen
X.509	Julkisen varmenteen rakenteen määrittelevä standardi (IETF)

## 1 JOHDANTO

Yhteiskunnan digitalisoituminen kasvattaa yksilön tarvetta erilaisille palveluille, ja näiden palveluiden käyttö vaatii käyttäjän vahvaa tunnistautumista. Jokaiseen palveluun suositellaan käyttämään eri salasanaa kuin muissa, sillä tämä vähentää palveluista mahdollisesti vuotavien tunnusten riskiä. Palveluiden ja yksittäisten tunnusten määrän kasvaessa ei usean salasanan muistaminen ole käyttäjäystävällistä. Edellä mainitusta syystä käyttää moni samaa salasanaa useassa palvelussa, vastoin suosituksia. Googlen arvion mukaan noin 17 % käyttäjistä käyttää samaa salasanaa uudelleen (Milka 2018). Luku on huolestuttava maailmalla tapahtuvien tietomurtojen takia. Vuonna 2016 Google keräsi 3,3 miljardia tunnusta noin 4 000 eri tietomurrosta. Näiden tunnusten joukossa oli 67 miljoonaa voimassa olevaa Google-salasanaa (Milka 2018). Suuret määrät tietomurroissa vuotaneita tunnuksia ovat luoneet tarpeen ongelman ratkaisemiseksi.

Salasanan hallintaohjelmat auttavat ihmisiä käyttämään eri salasanaa kaikille tunnuksille. Nämä ohjelmat pitävät kirjaa tunnuksista ja niiden salasanoista yhden pääsalasanan takana. Näin käyttäjän tarvitsee muistaa vain pääsalasana, jolla hän pääsee käsiksi muihin salasanoihinsa. Tämä helpottaa suosituksien seuraamista, kun muut salasanat voivat olla esimerkiksi salasanan hallintaohjelmien satunnaisesti generoimia. Näitä palveluita tarjoavat ilmaiseksi esimerkiksi Google, jolloin salasanojen hallinta on linkitetty Google tiliin. Tarjolla on myös maksullisia palveluita, joissa mukana saattaa tulla muitakin ominaisuuksia, kuten esimerkiksi sähköpostitilien reaaliaikaista uhkaseuranta tai salasanatietokantojen automaattista synkronointia. Mutta periaate pysyy samana, salasanat salataan yhden pääsalasanan taakse. Näin itse pääsalasana voidaan pitää turvallisena, kun muistettavana on vain yksi salasana. Pelkästään salasanan hallintaohjelmista voisi tehdä kokonaisen opinäytetyön, mutta tässä työssä niitä sivutaan osana monivaiheista tunnistautumista. Työssä keskitytään monivaiheiseen tunnistautumiseen, jonka kanssa salasanan hallintaohjelmat luovat vahvan perustan yksityishenkilön tietoturvalle. Salasanan hallintaohjelmia käydään läpi luvussa 7.

Monivaiheisen tunnistautumisen periaate on yksinkertainen, salasanan lisäksi vaaditaan yksi tai useampi tapa tunnistautumiseen ennen kuin kirjautuminen



palveluun hyväksytään. Näin luodaan toinen este ja pelkän salasanan vuotaminen ei riitä tunnuksen väärinkäyttöön. Monet yritykset ovat omaksuneet monivaiheisen tunnistautumisen osaksi tietoturvapoliittikaansa, joten tapa ei ole kaikille täysin vieras. Tästä huolimatta moni jättää monivaiheisen tunnistautumisen osaksi työtä eikä ota tapaa osaksi yksityiselämäänsä. Kuluttajien huonolle sopeutumiselle monivaiheiseen tunnistautumiseen on monia syitä, mutta näistä suurimpana nousee esiin ylimääräinen vaiva (Milka 2018). Nimensä mukaisesti monivaiheisessa tunnistautumisessa lisätään vaihe tunnistautumiseen, ja tämä parantaa tietoturvaa lisäämällä tunnistautumisten määrää. Aktiivisista Google tileistä alle 10 % oli ottanut käyttöön monivaiheisen tunnistautumisen (Milka 2018).

Tämän opinnäytetyön tarkoitus on madaltaa kynnystä monivaiheisen tunnistautumisen käyttöönotossa käymällä läpi suosituimpia vaihtoehtoja monivaiheisesta tunnistautumisesta ja niiden käyttöönotosta. Samalla käsitellään monivaiheisen tunnistautumisen hyödyt ja haasteet. Tavoitteena käyttäjäystävällinen ja helposti ymmärrettävä opinnäytetyö, josta olisi apua mahdollisimman monelle.

Opinnäytetyön lopuksi tehdään yhteenveto työstä ja sen tuloksista. Lisäksi pohditaan tulevaa ja esitetään mahdollisia jatkotutkimuksia.

## **2 TUTKIMUKSEN TOTEUTUS**

Opinnäytetyö toteutetaan kvalitatiivisella eli laadullisella tutkimusmenetelmällä. Tutkimuksessa analysoidaan asiantuntijakirjoituksia ja dokumentaatioita.

Opinnäytetyön aihe sai alkunsa kollegan ehdotuksesta ja henkilökohtaisesta havainnosta monivaiheistentunnistautumisen käyttämättömyydestä lähipiirissä. Työssä pureudutaan monivaiheiseen tunnistautumiseen, erilaisiin tunnisteisiin, sekä Suomessa yleisessä käytössä oleviin monivaiheisen tunnistautumisen menetelmiin. Tämä lisäksi työssä käydään lävitse yleisimpien palveluiden käyttöä.

Vaikka salasanan hallintaohjelmat eivät ole osa monivaiheista tunnistautumista, koettiin niiden käsittely tässä työssä hyödylliseksi. Salasanan hallintaohjelmista käytetään esimerkkinä ilmaista ja maksullista vaihtoehtoa. Näistä palveluista käydään lävitse niiden toiminnan ja käytön lisäksi turvallisuus, sekä salasanan hallintaohjelmiin liittyvät riskit.

## **2.1 Tutkimusongelma ja -kysymys**

Opinnäytetyön aihetta arvioidessa nousi esiin kaksi selkeää tutkimusongelmaa. Monivaiheisen tunnistautumisen käyttöönotto koetaan hankalaksi, ja se tuottaa käyttäjille ylimääräistä vaivaa. Lisäksi kaikille käyttäjille ei ole selvää miten monivaiheinen tunnistautuminen auttaa heitä suojaamaan tilejään ja sen kautta henkilökohtaisia tietojaan. Näiden kahden kohdan summa johtaa yleensä monivaiheisen tunnistautumisen käyttämättä jättämiseen, kun sen tuottamaa vaivaa ei koeta hyödylliseksi.

Tutkimuskysymyksen tulisi pureutua kumpaankin kohtaan, jotta käyttöönotto olisi mahdollisimman vaivatonta ja monivaiheisin tunnistautumisen hyödyt olisivat käyttäjille selkeät. Aiheena monivaiheinen tunnistautuminen on erittäin laaja, joten tässä opinnäytetyössä ei voida vastata kysymykseen jokaisen olemassa olevan menetelmän kohdalta.

Opinnäytetyössä keskitytään siis vain kirjoitushetkellä yleisimpiin monivaiheisen tunnistautumisen menetelmiin Suomessa. Näin tutkimuskysymykseksi muodostuu seuraava: Miten yleisimmät monivaiheisen tunnistautumisen menetelmät otetaan käyttöön ja mitkä ovat näiden hyödyt?

Tähän tutkimuskysymykseen vastaamalla voidaan laskea kynnystä monivaiheisen tunnistautumisen käyttöönottoon ja tuoda esiin monivaiheisen tunnistautumisen hyödyt sekä tärkeys nykymaailmassa.

## **2.2 Tutkimusmenetelmä**

Tutkimusmenetelmäksi tälle opinnäytetyölle valikoitui kvalitatiivinen eli laadullinen tutkimusmenetelmä. Tähän tutkimusmenetelmään päädyttiin punnitsemalla laadullisen ja määrällisen tutkimusmenetelmän eroja sekä sitä, miten kumpikin vastaa opinnäytetyön tavoitteita.

Määrällisessä tutkimuksessa tutkija käsittelee ja analysoi numeerista aineistoa. Tilastotieteiden avulla määrällisessä tutkimuksessa voidaan todentaa ja testata hypoteeseja (Lapin ammattikorkeakoulu 2021). Määrällisessä tutkimuksessa ollaan kiinnostuneita syy- ja seuraussuhteista, asioiden vertailusta sekä numeraalisesti esitettävien tuloksien selittämisestä (Jyväskylän yliopisto 2015).

Laadullisessa tutkimuksessa pyritään ymmärtämään tutkittavan kohteen laadullisia ominaisuuksia ja niiden merkitystä (Jyväskylän yliopisto 2015). Laadullisessa tutkimuksessa aineiston luonne eroaa määrällisen tutkimuksen aineistosta, jossa aineisto on enemmän numeerista. Laadullisessa tutkimuksessa aineisto voi olla havainto- ja dokumentaatiopohjaista. Laadullisen tutkimuksen tavoite on löytää tai paljastaa tosiasioita toisin kuin määrällisessä tutkimuksessa, jossa todennetaan jo olemassa olevia väittämiä (Hirsjärvi ym. 2009, 161). Laadullisessa tutkimuksessa päätelmien teossa yhdistyvät tutkijan oma intuitio, tulkinta, luokittelu- ja asioiden yhdistelytaidot. Koska jokainen tutkija tekee päätöksiä omalla tapaa, voi samasta aineistosta tehdä useita eri päätelmiä eri tutkijoiden välillä (Metsämuuronen 2006, 82).

Näitä tutkimusmenetelmiä punnitessa todettiin kvalitatiivisen eli laadullisen tutkimuksen palvelevan opinnäytetyön tarpeita. Tässä opinnäytetyössä käytävä materiaali ei ole numeraalista ja pelkästään tutkimusongelma tuo ilmi, että yhtenä muuttuvana tekijänä on ihminen. Näin saadaan eliminointua määrällinen eli kvantitatiivinen menetelmä pois vaihtoehtoista ja päädytään laadulliseen tutkimusmenetelmään.

### **3 MONIVAIHEINEN TUNNISTAUTUMINEN**

Monivaiheinen tunnistautuminen on prosessi, jossa käyttäjää pyydetään varmentamaan henkilöllisyytensä kahteen tai useampaan kertaan ennen sisäänkirjautumista (Kyberturvallisuuskeskus 2021). Monivaiheisessa tunnistautumisessa voidaan käyttää useita tapoja. Näitä yksilöiviä tunnisteita ovat: ”jotain mitä tiedät”, ”mitä omistat” tai ”missä olet” (Cisco 2020). Näiden lisäksi viime vuosina ovat yleistyneet ”jotain mitä olet” eli biometriset tunnisteet, kuten sormenjälki (Kyberturvallisuuskeskus 2021).

Hyvä esimerkki monivaiheisesta tunnistautumisesta on rahan nostaminen pankkiautomaatista. Rahan nostaminen vaatii ”jotain mitä omistat” eli tässä tapauksessa pankkikorttisi. Tämän lisäksi tarvitaan ”jotain mitä sinä tiedät” eli tunnuslukusi (Cisco 2020). Näiden kahden tiedon täsmätessä pääsee käyttäjä nostamaan rahaa pankkitililtä, muussa tapauksessa pääsy tilille evätään.

Nykypäivänä perinteinen käyttäjätunnus-salasanayhdistelmä tarjoaa suhteellisen heikon turvan käyttäjälle. Tämä johtuu inhimillisistä rajoitteista muistaa ja käyttää useampaa salasanaa eri palveluissa. Tämä saakin monet käyttämään samaa salasanaa useammassa paikassa tai laskemaan useamman salasanan monimutkaisuutta muistamisen helpottamiseksi. Salasanat ovat myös alttiita tietomurroilla, kalasteluille ja haittaohjelmille. (Cisco 2020.)

Kun käyttäjällä on käytössään monivaiheinen tunnistautuminen, ei pelkkä käyttäjätunnuksen ja salasanan vuotaminen riitä käyttäjätilin kaappaamiseen (Kyberturvallisuuskeskus 2021). Monivaiheisella tunnistautumisella voidaan estää jopa 99,9 % tilien kaappausyrityksistä (Microsoft 2019).

### **3.1 Tunnistetyypit**

Henkilön yksilöivät tunnisteet on jaettu neljään kategoriaan, joita ovat: ”jotain mitä tiedät”, ”jotain mitä omistat”, ”missä olet” ja ”jotain mitä olet”. Eri kategoriat tarjoavat tunnisteiden eri tilanteisiin. Tunnisteiden valintaa voivat rajoittaa tietyt teknologiset vaatimukset tai tunnisteiden käyttöönottoon vaadittu teknologinen tietotaito. Eri tunnisteilla on omat hyötynsä, mutta niiden tuomat riskit on otettava myös huomioon.

### **3.2 Jotain mitä tiedät**

”Jotain mitä tiedät” kattaa perinteisen käyttäjätunnus-salasanayhdistelmän. Nykypäivänä tämän yhdistelmän lisäksi olisi hyvä olla jokin muista tunnistetyypeistä (Microsoft 2021d.) Salasanojen vaatimuksien ja kirjautumisten määrien noustessa ajautuvat käyttäjät luomaan yksinkertaisempia salasanoja, joita käytetään useammassa paikassa. Tieto voidaan myös unohtaa, ja mikäli sitä säilytetään jossain, voidaan se varastaa (Cisco 2020).

### 3.3 Jotain mitä omistat

”Jotain mitä omistat” viitataan johonkin fyysiseen esineeseen. Näitä tunnisteita voivat olla muun muassa älypuhelimessa käytettävät applikaatiot, tunnuslukulaitteet, SMS-välityksellä saapuvat OTP-kertakäyttösalasana, tunnistautumiseen tarkoitetut USB-laitteet ja U2F-standardin mukaiset turva-avaimet (AWS 2021). Näiden tunnisteiden hyötynä on niiden vaikea huijattavuus. Älypuhelimien käyttö on yleistynyt monivaiheisessa tunnistautumisessa niiden saatavuuden vuoksi useimmissa tilanteissa. Kääntöpuolena tälle on se, että fyysiset laitteet ovat alttiita varkaudelle tai niiden kadottamisille (Cisco 2020).

### 3.4 Missä olet

”Missä olet” ovat lokaatiopohjaisia tunnisteita. Monivaiheisessa tunnistautumisessa voidaan käyttäjän sijainti määritellä GPS-koordinaateilla, verkkosijainnilla tai laitteen tunnistamisella. Esimerkiksi kulkukortilla ovesta kuljettaessa voidaan verkkosijainnin perusteella tunnistaa, onko kyseisen kulkukortin omistajan työpuhelin oven lähettyvillä ennen lukituksen avausta. Näiden tunnisteiden hyötynä on niiden minimaalinen käyttäjältä tarvittava syöte, joka ei häiritse käyttäjän tuottavuutta. Näiden tunnisteiden käyttöönotto vaatii kuitenkin teknistä osaamista (Cisco 2020).

### 3.5 Jotain mitä olet

”Jotain mitä olet” eli biometriset tunnisteet. Näihin kuuluvat muun muassa sormenjäljen tunnistus, kasvojen tunnistaminen tai silmän retinan ja iiriksen tunnistaminen. Nämä uniikit tunnisteet ovat aina saatavilla ja turvassa, jonka takia tämä tunnistekategoria on erityisen vakuuttava. Teknologian kehittyessä voi näiden tunnisteiden joukkoon liittyä muita uniikkeja tunnisteita, jotka ovat aina mukana. Esimerkkinä näistä on kämmenen verisuonien käyttäminen tunnisteena. Kämmen verisuonet luetaan käyttäen infrapunavaloa ja tulosten perusteella luodaan uniikki biometrinen tunniste. Kehon sisäisen tunnisteiden kopiointi on huomattavasti vaikeampaa. Biometristen tunnisteiden vaatimus onkin niiden käyttöä mahdollistava teknologia, jota ei ole kaikilla saatavissa (Cisco 2020.) Tällaiset uniikit ja muokkaamattomat tunnisteet tuovat muka-

naan kuitenkin riskejä. Mikäli tietovuodon yhteydessä vuotaa biometrisiä tunnisteita, on käyttäjien identiteetti vaarassa. Näiden tunnisteiden väärinkäyttö voi johtaa vakaviin seuraamuksiin, ja tunnisteita on vaikea kiistää.

## **4 MOBIILIVARMENNE**

Mobiilivarmenne on SIM-kortissa sijaitseva tunniste, jota voidaan käyttää vahvassa tunnistautumisessa verkkopalveluihin tai muuhun sähköiseen asiointiin. Mobiilivarmenneen käyttö vaatii tällä tunnisteella varustetun SIM-kortin, näitä SIM-kortteja tarjoavat Suomessa tällä hetkellä DNA, Elisa ja TeliaSonera (Mobiilivarmenne 2020c).

Mobiilivarmenne toimii yli 20 000 palvelussa ja käyttäjiä on yli 200 000 (Mobiilivarmenne 2020c). Suomalaiset mobiilioperaattorit muodostavat luottamusverkoston, johon kuuluvat kaikki mobiilivarmennetta tarjoavat asiointipalvelut ja mobiilivarmenneen käyttäjät. Käyttäjien on mahdollista käyttää kaikkien luottamusverkkoon kuuluvien palveluntarjoajien palveluita riippumatta operaattorista (DNA 2020).

### **4.1 Käyttöönotto**

Mobiilivarmenneen käyttöönotto tapahtuu oman mobiilioperaattorin portaalin kautta. Linkit ovat helposti saatavissa [www.mobiilivarmenne.fi](http://www.mobiilivarmenne.fi)-verkkosivulta. Koska käyttöönotto tapahtuu jokaisen mobiilioperaattorin omassa portaalissa, on käyttöliittymä hieman erilainen riippuen käyttäjän mobiilioperaattorista.

Käyttöönotto vaatii operaattorista riippumatta ensitunnistautumisen, jota verrataan Väestörekisterikeskuksen tietokantaan. Sähköisissä kanavissa tämä tarkoittaa kuluttajan verkkopankkitunnuksia. Mikäli tiedot eivät täsmää, ei ensitunnistautumista voida varmentaa eikä täten mobiilivarmennetta myöntää (DNA 2020).

Elisan asiakkailla on mahdollisuus ottaa mobiilivarmenne käyttöön myös Elisan myymälöissä. Tällöin ensitunnistautumiseen vaatimukset ovat samat, eli henkilön ensitunnistautumiseen esitettyjen henkilöllisyysasiakirjojen tietojen täytyy täsmätä Väestörekisterikeskuksen tietokantaan. Hyväksyttäviä henkilöllisyysasiakirjoja ovat muun muassa voimassa oleva suomalainen passi tai

2011 jälkeen myönnetty voimassa oleva suomalainen henkilökortti (Elisa 2020). Telia tarjoaa myös mahdollisuuden mobiilivarmenteen käyttöönotolle Telia Kaupassa. Ensitunnistautumisen vaatimukset ovat samat kuin Elisalla, eli voimassa olevien henkilöllisyysasiakirjojen tietojen on täsmättävä Väestörekisterikeskuksen tietokantaan (Telia 2020).

Mobiilivarmenteen käyttöönoton yhteydessä käyttäjä valitsee itselleen tunnusluvun, jolla suojataan varmenteisiin liittyvät yksityiset avaimet SIM-kortilta (Elisa 2020).

## 4.2 DNA

DNA Mobiilivarmenteen käyttöönotto vaatii soveltuvan SIM-kortin, verkkopankkitunnukset ja käyttäjän tulee olla vähintään 15-vuotias. DNA Mobiilivarmenteen rekisteröinti tapahtuu osoitteessa <https://www.dna.fi/mobiilivarmenne>.

Mobiilivarmenteen käyttöönotto alkaa henkilöllisyyden varmistuksella. Tämä tapahtuu kirjautumalla sisään verkkopankkitunnuksilla. Onnistuneen tunnistautumisen jälkeen kuvassa 1 syötetään liittymän puhelinnumero, jolle mobiilivarmenne halutaan aktivoida.

**DNA** **Mobiilivarmenne**

1 Tunnistautuminen 2 Luo tunnistautumisavain 3 Luo allekirjoitusavain

**Syötä seuraavaksi puhelinnumerosi**

Mobiilivarmenne liitetään matkapuhelimesi SIM-korttiin.

Anna puhelinnumero, johon haluat liittää mobiilivarmenteen:

Puhelinnumero \*

JATKA

Kuva 1. DNA Mobiilivarmenne puhelinnumero (Mobiilivarmenne 2020a)

DNA lähettää käyttäjälle vahvistusviestin syötettyyn puhelinnumeroon. Vahvistusviestissä oleva vahvistuskoodi syötetään kuvan 2 aktivointisivun vahvistuskoodi kohtaan.

Kuva 2. DNA Mobiilivarmenne tarkistus (Mobiilivarmenne 2020a)

Kun käyttäjän henkilöllisyys ja puhelinnumero on tarkistettu, ohjataan käyttäjä luomaan itselleen mobiilivarmenteen tunnistusavain kuvassa 3. Tunnistusavain on 4–8 merkin numerosarja ja se luodaan laitteella, jossa liittymän SIM-kortti on asennettuna.

Kuva 3. DNA Mobiilivarmenne tunnusluvunluonti (Mobiilivarmenne 2020a)

Tämän jälkeen käyttäjä luo itselleen vielä mobiilivarmenteen allekirjoitusavaimen. Tätä avainta voidaan käyttää digitaaliseen allekirjoitukseen ja luonti tapahtuu laitteelta, johon SIM-kortti on asennettuna. Mobiilivarmennetta voi testata DNA Mobiilivarmenteen hallintapaneelissa. (Mobiilivarmenne 2020a.)



### 4.3 Elisa

Elisa Mobiilivarmenteen käyttöönotto verkossa vaatii käyttäjältä vähintään 15 vuoden iän, verkkopankkitunnukset ja Elisan liittymän soveltuvalla SIM-kortilla. Sähköinen aktivointi tapahtuu verkossa <https://www.elisa.fi/varmenne>. Elisa tarjoaa myös mahdollisuuden mobiilivarmenteen aktivointiin Elisa myymälöissä. Tällöin henkilöllisyys on todistettava henkilöllisyysasiakirjoilla, joiden tiedot täsmäävät Väestörekisterikeskuksen tietokantaan. (Mobiilivarmenne 2020b).

Aktivoinnin alussa syötetään kuvan 4 kenttään liittymän puhelinnumero. Elisa lähettää syötettyyn puhelinnumeroon kertakäyttöisen salasanan, joka syötetään alla olevaan kenttään. Näin varmistetaan, että liittymälle on mahdollista aktivoida Elisa Mobiilivarmenne ja että käyttäjä on syöttänyt oikean puhelinnumeron.

1/6

Liittymän kelpoisuus

Anna puhelinnumerosi, johon lähetämme kertakäyttösalasanan varmistaaksemme, että liittymäsi voi rekisteröidä Elisa Mobiilivarmenteen.

050123456 ✓

LÄHETÄ SALASANA

Saat puhelimeesi kertakäyttösalasanasi hetken kuluttua.

Kertakäyttösalasana \*

VAHVISTA SALASANA

Kuva 4. Elisa Mobiilivarmenne liittymän kelpoisuus (Mobiilivarmenne 2020b)

Kun liittymän kelpoisuus on tarkistettu onnistuneesti, tunnistautuu käyttäjä verkkopankkitunnuksillaan ja hyväksyy Elisa Mobiilivarmenteen sopimusehdot. Tämän jälkeen käyttäjä syöttää kuvan 5 kenttiin omat yhteystietonsa.

**Yhteystiedot**

Anna alla oleviin kenttiin omat yhteystietosi.

Matti	✓
Meikäläinen	✓
Ratavartijankatu 25	✓
00520	✓
Helsinki	✓
050123456	✓
matti.meikalainen@elisa.fi	✓

Kuva 5. Elisa Mobiilivarmenne yhteystiedot (Mobiilivarmenne 2020b)

Yhteystietojen syöttämisen jälkeen käyttäjä luo itselleen kuvan 6 mukaisesti mobiilivarmenteen tunnusluvun, sekä erillisen allekirjoitus-tunnusluvun. Mobiilivarmenteen tunnusluvulla kirjaudutaan sisälle sähköisiin palveluihin ja allekirjoitus-tunnusluvulla voidaan allekirjoittaa sähköisiä asiakirjoja käyttäen mobiilivarmennetta.

**Tunnusluku:**

Tunnusluvulla tunnistaudut sähköisissä palveluissa

•••• ✓

Pituus vähintään 4 ja enintään 8 numeroa

•••• ✓

☐ Näytä tunnusluku

**Allekirjoitus-tunnusluku:**

Allekirjoitus-tunnusluvulla teet sähköisiä allekirjoituksia palveluissa

•••••• ✓

Pituus vähintään 6 ja enintään 8 numeroa

•••••• ✓

☐ Näytä allekirjoitus-tunnusluku

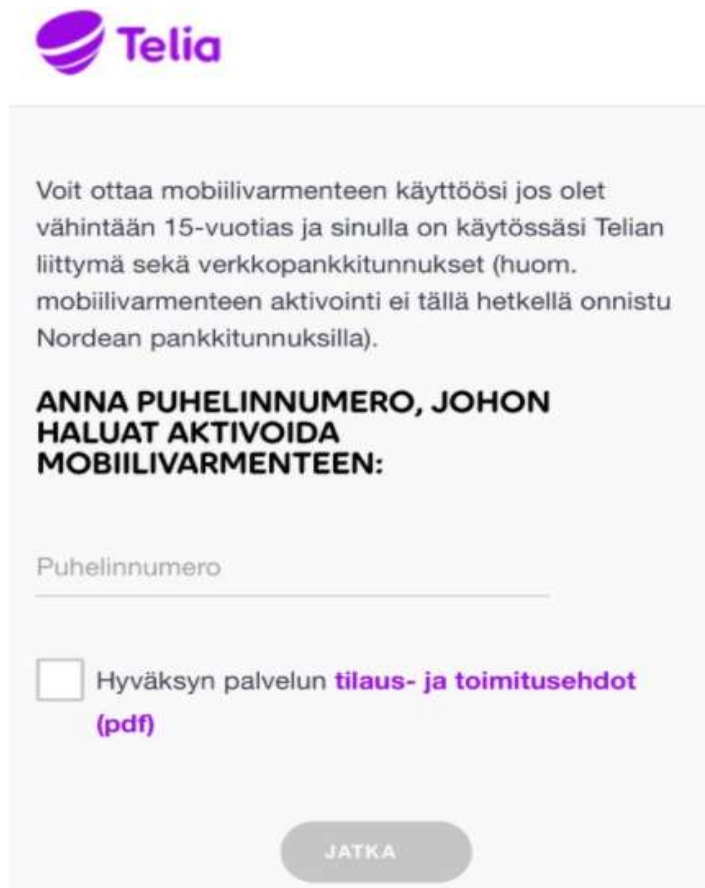
Kuva 6. Elisa Mobiilivarmenne tunnusluvut (Mobiilivarmenne 2020b)


Lopuksi vahvistetaan Elisa Mobiilivarmenteen rekisteröinti, jonka jälkeen käyttäjälle lähetetään viesti onnistuneesta rekisteröinnistä. Vahvistusviestin saavuttua on mobiilivarmenne valmiina käyttöön (Mobiilivarmenne 2020b).

#### 4.4 Telia

Telia Mobiilivarmenteen käyttöönotto verkossa vaatii käyttäjältä verkkopankkitunnukset, Telian liittymän ja vähintään 15 vuoden iän. Käyttöönotto verkossa tapahtuu verkkosivulta [telia.fi/mobiilivarmenne](https://telia.fi/mobiilivarmenne). Telia Mobiilivarmenne on myös mahdollista ottaa käyttöön Telia Kaupassa. Tässä tapauksessa verkkopankkitunnusten sijaan käyttäjän on todistettava henkilöllisyytensä virallisella henkilöllisyystodistuksella. Henkilöllisyystodistuksen tietojen on täsmättävä Väestörekisterikeskuksen tietokantaan.

Aluksi syötetään liittymän puhelinnumero, johon mobiilivarmenne halutaan aktivoida. Samalla käyttäjän on hyväksyttävä kuvan 7 mukaisesti Telia Mobiilivarmenteen tilaus- ja toimitusehdot.





Voit ottaa mobiilivarmenteen käyttöösi jos olet vähintään 15-vuotias ja sinulla on käytössäsi Telian liittymä sekä verkkopankkitunnukset (huom. mobiilivarmenteen aktivointi ei tällä hetkellä onnistu Nordean pankkitunnuksilla).

**ANNA PUHELINNUMERO, JOHON HALUAT AKTIVOIDA MOBIILIVARMENTEEN:**

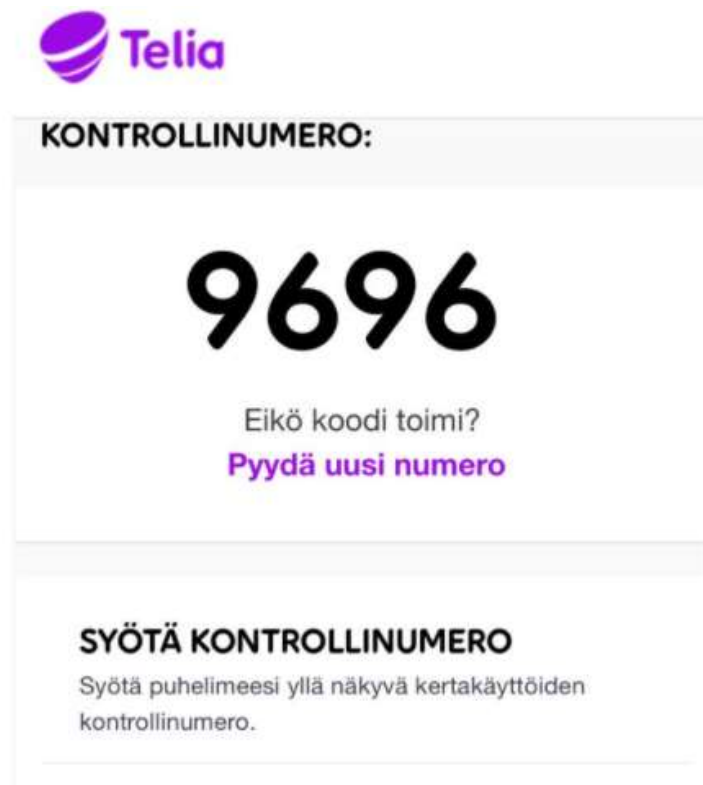
Puhelinnumero

☐ Hyväksyn palvelun **tilaus- ja toimitusehdot (pdf)**

**JATKA**

Kuva 7. Telia Mobiilivarmenne puhelinnumero (Mobiilivarmenne 2020d)

Mikäli liittymän SIM-kortille on mahdollista aktivoida mobiilivarmenne, pyydetään käyttäjää tunnistautumaan verkkopankkitunnuksilla. Onnistuneen tunnistautumisen jälkeen ohjeistetaan käyttäjää tunnusluvun luonnissa. Telia Mobiilivarmenteen aktivointisivulla näkyy kuvan 8 mukaisesti kontrollinumero. Kontrollinumerolla vastataan Telialta lähetettyyn tunnistuskyselyyn. Tunnistuskysely lähetetään viestillä puhelinnumeroon, jolle mobiilivarmennetta ollaan aktivoimassa.



Kuva 8. Telia Mobiilivarmenne kontrollinumero (Mobiilivarmenne 2020d)

Kun kontrollinumero on vahvistettu, pyydetään käyttäjää luomaan itselleen 4–8-numeroinen tunnusluku ja vahvistamaan se syöttämällä sama tunnusluku uudelleen. Onnistuneen tunnusluvun luonnin jälkeen käyttäjä saa viestillä vahvistuksen mobiilivarmenteen onnistuneesta rekisteröinnistä. Tämän jälkeen Telia Mobiilivarmenne on valmiina käyttöön. (Mobiilivarmenne 2020d.)

#### 4.5 Käyttö

Mobiilivarmenteen käyttö tapahtuu puhelimella, johon tunnisteiden omaava SIM-kortti on asennettu. Tunnistautumisen yhteydessä kirjautumissivulle syötetään käyttäjän puhelinnumero. Tämän jälkeen puhelimen ruudulle ilmestyy tunnis-

tautumispyyntö, jonka hyväksymisen jälkeen syötetään valittu tunnusluku. Mikäli tunnusluku täsmää mobiilivarmenteelle asetettua tunnuslukua, sallitaan käyttäjän kirjautuminen palveluun. (Mobiilivarmenne 2020c.)

#### **4.6 Mobiilivarmenteen tekniset tiedot**

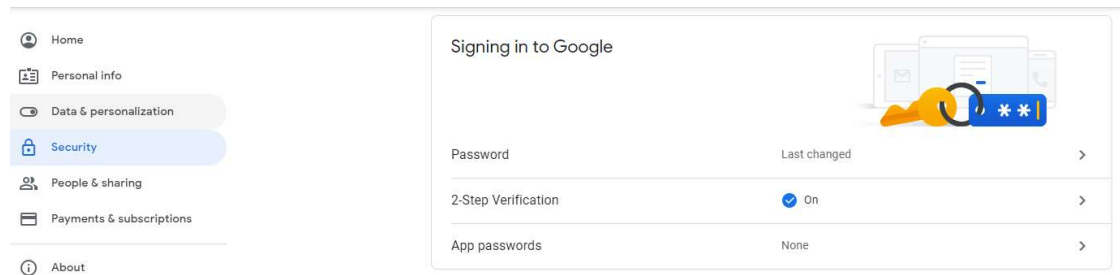
Mobiilivarmenne käyttää julkisen avaimen salausmenetelmää sekä X.509-varmenteita. Varmenteisiin sidotut yksityiset avaimet säilötään SIM-kortilla tunnusluvulla suojattuna (DNA 2020). Varmennepolitiikan mukaan käytetyt RSA-avainparit ovat vähintään 1024-bittisiä (Elisa 2014). Mobiilivarmenne noudattaa X.509 v.3-standardin suositusta. Sähköiset asiointitunnukset tallennetaan Subject-kentän SerialNumber-attribuuttiin ja käyttäjän SIM-kortin ICCID eidSmartCardSerialNumber -attribuuttiin (DNA 2020).

### **5 GOOGLE**

Googlen tarjoaa suuren määrän palveluita, jotka ovat kaikki mahdollista yhdistää yhdelle Google-tilille. Google-tilillä on mahdollista myös kirjautua joihinkin muiden palveluntarjoajien palveluihin. Tämä helpottaa monen arkea, kun pääsy useisiin palveluihin on yhden tilin kautta. Näin ollen kyseisen tilin suojaus on kuitenkin erittäin tärkeää etenkin, jos tilille on yhdistetty maksukortteja. Monivaiheinen tunnistautuminen on nopea tapa suojata tilinsä joutumista väärin käsiin.

## 5.1 Käyttöönotto

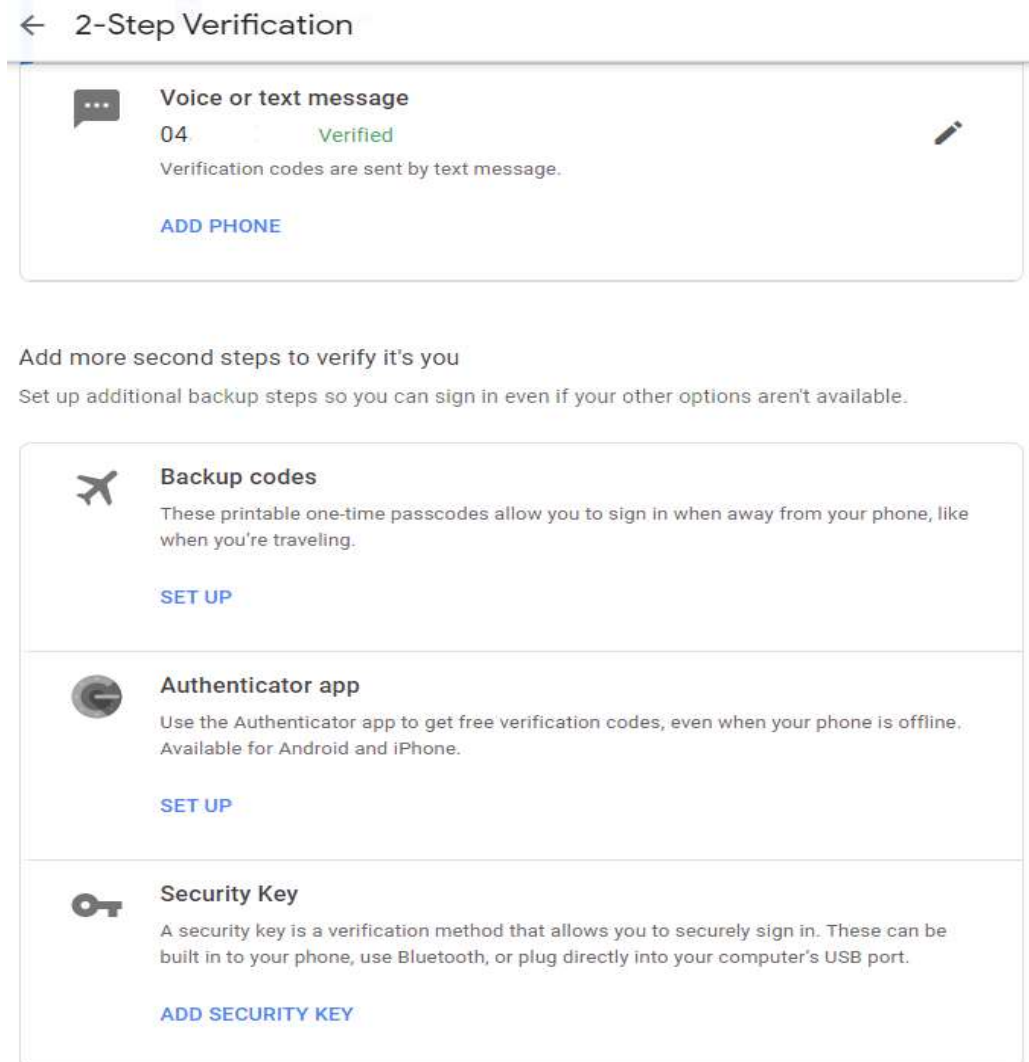
Googlen kuluttajalle tarjoama monivaiheinen tunnistautuminen käyttää ”jotain mitä tiedät” ja ”jotain mitä sinulla on” tunnistetyppejä (ks. Google 2021). Kaksivaiheisen tunnistautumisen saa otettua käyttöön Google-tilin asetuksista navigoimalla ”Suojaus/Security”-välilehdelle kuvan 9 mukaisesti. Suojaus-välilehdeltä voi asettaa palautuspuhelinnumeron tai -sähköpostin ja tarkkailla tilille tehtyjä kirjautumisia.



Kuva 9. Google kaksivaiheinen tunnistautuminen (Google 2021)

Oletuksena Googlen kaksivaiheisessa tunnistautumisessa on käytössä Google-kehotteet. Kehotteet ovat helpoin tapa käyttää kaksivaiheista tunnistautumista, mutta halutessasi voit vaihtaa tunnistautumistapaa Google-tilin asetuksista. Kehotteet lähetetään Android-puhelimelle, jolla on kirjaututtu sisään Google-tilille. iPhone-puhelimilla käytössä pitää olla Google- tai Gmail-sovellus, jolla on kirjaututtu Google-tilille. (Google 2021.)

Google-kehotteiden lisäksi voidaan monivaiheisena tunnisteena käyttää suojausavaimia, vahvistuskoodeja puhelun välityksellä tai tekstiviestillä sekä autentikointisovelluksia kuten Google Authenticator (Google 2021). Tunnisteita pääsee muokkaamaan Suojaus-välilehdeltä. Kuvassa 10 esitellään kaksivaiheisen tunnistautumisen valikko.



Kuva 10. Google kaksivaiheisen tunnistautumisen vaihtoehtoja (Google 2021)

## 5.2 Käyttö

Oletuksena toisena tunnistautumistapana on käytössä Googlen suosittelemat älypuhelinkehotteet. Kehotteiden ollessa käytössä lähettää Google salasanan syöttämisen jälkeen kehotteen älypuhelimeen. Kehotteesta voidaan sallia tai estää kirjautuminen perustuen kehotteen ilmoittamiin tietoihin. Kehotteessa ilmoitetaan laite, jolla kirjautumista yritetään ja laitteen sijainti (Google 2021.)

Mikäli käytettäväksi toisen vaiheen tunnistautumistavaksi on valittu soitto tai tekstiviesti, kysytään kirjautumisen yhteydessä kuusimerkkistä koodia. Koodi toimitetaan käyttäjälle tekstiviestillä tai soittaen, riippuen valitusta menetelmästä. (Google 2021.)

Turva-avaimet ovat esineitä, joissa on jonkin teknologian mahdollistama tunnistautumismenetelmä. Näitä tunnistautumismenetelmiä voivat olla puhelimen Bluetooth, erinäiset USB-porttiin liitettävät laitteet tai erilaiset NFC-avaimet. Kirjautumisen yhteydessä pyydetään toisena varmenteena turva-avainta. Mikäli puhelimen Bluetooth toimii turva-avaimena, on molemmissa laitteissa oltava Bluetooth päällä tunnistautumisen onnistumiseksi. (Google 2021.)

Google Authenticator tarjoaa kertakäyttöisiä aikarajoitettuja tunnistekoodoja. Sovellus on saatavilla puhelimen sovelluskaupoista App Store ja Google Play. Sovelluksen avautuessa opastetaan käyttäjää tunnistekoodien käyttöön-otossa. Tunnistautumisen yhteydessä syötetään sovelluksessa näkyvillä oleva koodi. Tämä mahdollistaa monivaiheisen tunnistautumisen myös silloin, kun puhelimessa ei ole muuta yhteyttä. Tälle tunnistusmenetelmälle on mahdollista käyttää muita sovelluksia kuin Googlen Authenticator, kunhan siinä on saatavilla aikarajoitettuja tunnistekoodoja. Vastapainoisesti Google Authenticatoria voidaan käyttää muillakin kuin Google-tileillä, kunhan tilit tukevat aikarajoitettuja tunnistekoodoja. (Google 2021.)

## **6 MICROSOFT**

Microsoftin kehittämä ja laajasti levinnyt Windows-käyttöjärjestelmä nauttii suurta markkinaosuutta. Käyttöjärjestelmän uusin Windows 10-versio suosittelee asennuksen yhteydessä käyttäjiä yhdistämään Microsoft-tilinsä Windows 10 -käyttöjärjestelmään. Microsoft-tilin tunnuksia voidaan käyttää sisään kirjautumiseen muissa Windows-laitteissa ja Microsoftin tarjoamissa palveluissa. Tästä johtuen Microsoft-tilin suojaus on erittäin tärkeää, sillä tilin vaarantuminen vaarantaa käyttäjän kaikki siihen yhdistämät laitteet ja palvelut.

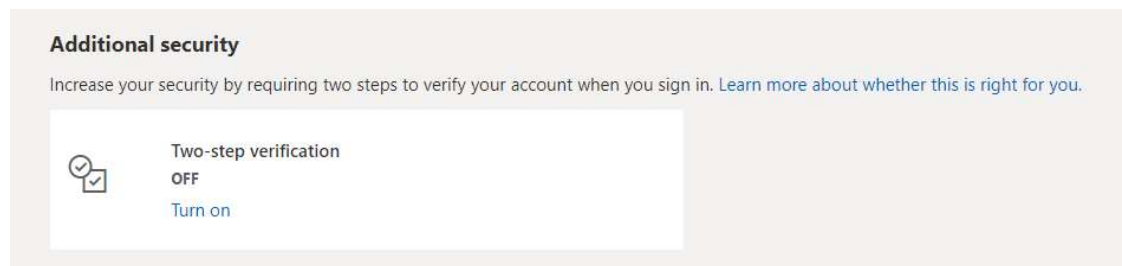
Windows Hello tarjoaa yksilöidyn ja nopean kirjautumisen Windows 10-laitteille. Kirjautumiseen voidaan käyttää PIN-koodia, kasvojen tunnistusta siihen sopivalla kameralla tai sormenjäljen tunnistusta sormenjäljenlukijalla. PIN-



koodi täytyy asettaa kaikkien vaihtoehtojen käyttöönoton yhteydessä. Tämä PIN-koodi on sidottu vain kyseiseen laitteeseen ja sen varmuuskopio on liitetty käyttäjän Microsoft-tiliin.

## 6.1 Käyttöönotto

Microsoft tarjoaa kuluttajakäyttäjille monivaiheiseen tunnistautumiseen Microsoft Authenticator -sovelluksen älypuhelimille. Microsoft Authenticator -sovellus on ladattavissa Google Play- ja App Store-sovelluskaupoista. Monivaiheisen tunnistautumisen saa otettua käyttöön kuvan 11 mukaisesti Microsoft-tilin turvallisuusasetuksista. (Microsoft 2021c.)



Kuva 11. Microsoft turvallisuusasetukset kaksivaiheinentunnistautuminen (Google 2021)

Kaksivaiheisen tunnistautumisen käyttöönotossa seurataan Microsoftin vaiheittaista ohjeistusta. Käyttöönoton yhteydessä ladataan Microsoft Authenticator -sovellus älypuhelimelle ja linkitetään se omaan Microsoft-tiliin. Kun sovellus on linkitetty omaan Microsoft-tiliin kuva 12, on kaksivaiheinen tunnistautuminen käytössä heti.



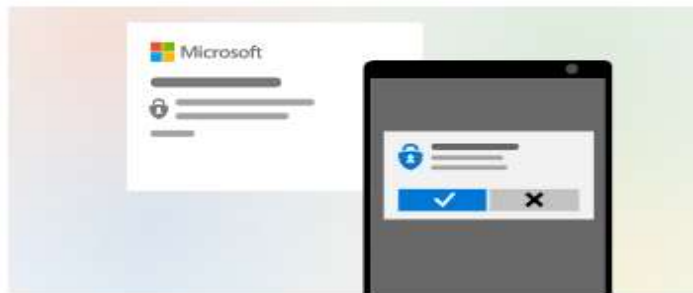
Kuva 12. Microsoft kaksivaiheinen tunnistautuminen otettu käyttöön (Microsoft 2021)

## 6.2 Käyttö

Microsoft Authenticator -sovelluksen ollessa käytössä lähettää Microsoft kehotteen sovellukseen kirjautumisen yhteydessä. Kehotteesta voidaan sallia tai estää kirjautumisyritys. Näin ollen jonkun muun yrittäessä kirjautua Microsoft-tilillesi tulee siitä ilmoitus älypuhelimeen ja pääsy voidaan evätä. Kirjautuessa Microsoft-tilille uudella laitteella tai uudesta sijainnista täytyy pelkän kehotteen lisäksi valita kuvan 13 mukaisesti Microsoft Authenticator sovelluksesta kirjautumissivulla näytettävä numero. (Microsoft 2021b.)

### Check Microsoft Authenticator

36 In your Microsoft Authenticator app, tap the number here to sign in.



☐ Keep me signed in

[Other ways to sign in](#)

Kuva 13. Microsoft kaksivaiheinen tunnistautuminen käytössä (Microsoft 2021)

Microsoft Authenticator -sovellus on oletuksella lukittu käyttämään älypuheli-  
men lukitusta. Tämä voi siis olla PIN-koodi, sormenjälki tai kasvojentunnistus.  
Microsoft Authenticator tarjoaa myös standardin mukaisen aikarajoitetun ker-  
takäyttöisen pääsykoodin. Tämän takia Microsoft Authenticator -sovellukseen  
voidaan linkittää muitakin kuin Microsoft-tiliä, kunhan tilit itsessään tukevat  
pääsykoodin käyttöä. (Microsoft 2021a.)

## 7 SALASANAN HALLINTAOHJELMISTOT

Kun jokaiseen palveluun suositellaan käytettäväksi aina eri salasanaa, saavu-  
tetaan nopeasti sellainen määrä salasanoja, joiden muistaminen tuottaa käyt-

täjille vaikeuksia. Tämä ilmiö on luonut markkinoille tarvetta salasanojen hallintaohjelmistoille. Näiden tarkoitus on helpottaa eri salasanan käyttöä jokaisessa palvelussa. Vaikka nämä ohjelmistot eivät suoraan liity monivaiheiseen tunnistautumiseen, käydään niitä läpi tässä opinnäytetyössä niiden merkittävien hyötyjen takia.

## **7.1 KeePass**

KeePass on ilmainen avoimen lähdekoodin salasananhallintaohjelma, joka on saatavilla tietokoneelle. Koska KeePass on avoimen lähdekoodin ohjelma, löytyy siitä useita sovituksia esimerkiksi Androidille ja iOS:lle.

KeePass toimii salasanojen tietokantana, jonne salasanat salakirjoitetaan ja ne suojataan yhdellä pääsalasanalla. Näin käyttäjä voi käyttää jokaiselle tilille uniikkia salasanaa muistamalla vain pääsalasanan. Tämä parantaa käyttäjän tietoturvaa, sillä yhden salasanan vuotaminen ei vaaranna kaikkia tilejä. KeePass voi toimia myös täysin kannettavassa muodossa, se voidaan asentaa USB-tikulle ja ei vaadi asennusta toimiakseen Windows -työasemilla. (KeePass 2021.)

### **7.1.1 Turvallisuus**

Tietokannan salaamiseksi KeePass käyttää AES-256- ja Twofish-salausalgoritmeja. KeePass ei salaa pelkästään salasanoja vaan kaiken tietokannassa olevan tiedon. AES-256 luokitellaan erittäin turvalliseksi salausalgoritmiksi. AES-256 on Yhdysvaltojen standardi salausalgoritmi, ja se on saanut Kansallisen turvallisuusviraston (NSA) hyväksynnän huippusalaiselle informaatiolle. Pääsalasana ja siihen liittyvien komponenttien hajauttamiseen käytetään SHA-256 tiivistefunktiota. SHA-256 vastaan ei ole tiedossa olevia hyökkäyksiä. (KeePass 2021.)

KeePassin ollessa käynnissä pidetään herkäksi luokitellut tiedot salattuna prosessimuistissa. Näihin tietoihin kuuluvat pääsalasana ja tietokantaan säilötyt salasanat. Käyttäjänimiä, liitteitä tai muistiinpanoja ei ole salattu prosessimuistissa. Tämän ansiosta vaikka prosessimuisti tallennettaisiin, ei sieltä löydy selväkielisiä salasanoja. (KeePass 2021.)

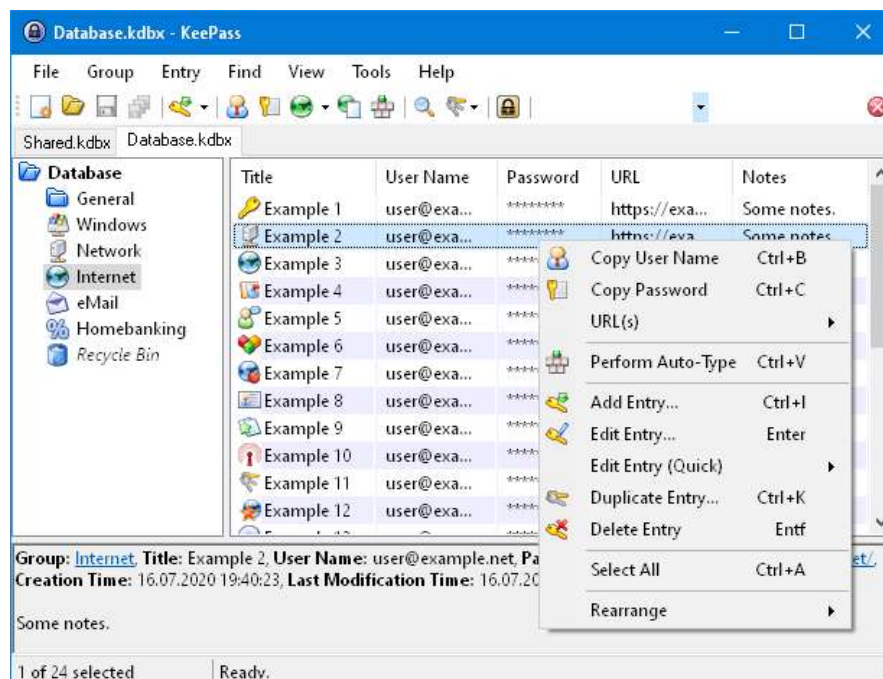
### 7.1.2 Käyttö

Kun KeePass otetaan käyttöön ensimmäistä kertaa, pyydetään käyttäjää valitsemaan pääsalasana, jolla tietokanta salataan. Tämän jälkeen tietokantaa avattaessa kysytään kuvan 14 mukaisesti käyttäjältä kyseisen tietokannan pääsalasanaa ennen tietokannan avaamista.



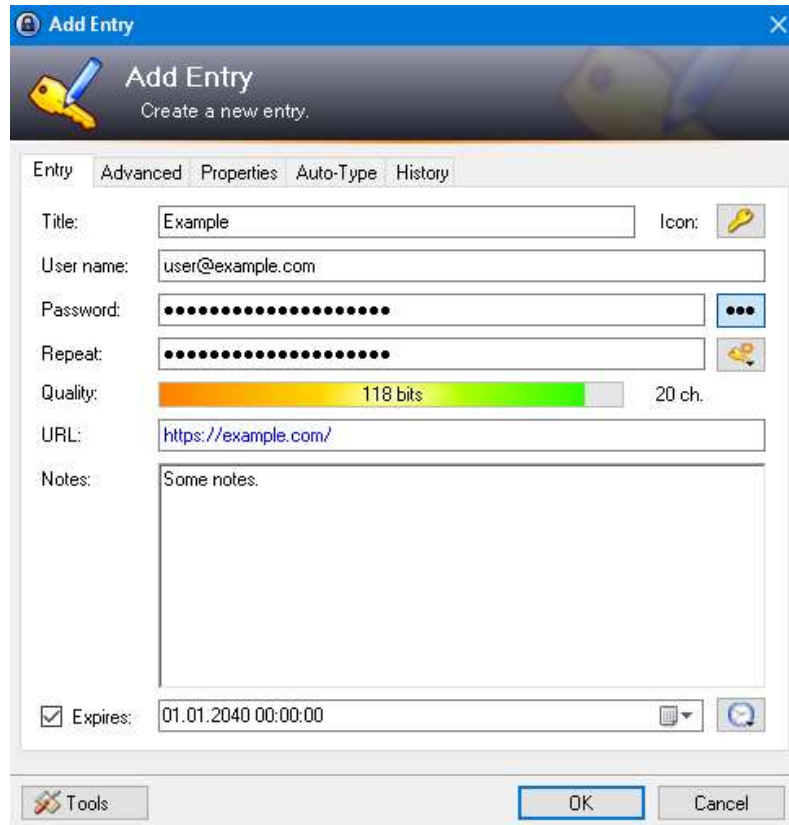
Kuva 14. KeePass tietokannan avaaminen pääsalasanalla (KeePass 2021)

KeePassin kanssa voidaan käyttää useita eri tietokantoja. Tällöin eri tietokannat aukeavat välilehtinä ja niiden välillä on helppo liikkua. Tietokannassa käyttäjän tunnukset ja salasanat on listattu yksittäisinä merkintöinä kuvan 15 tapaan ja haku ominaisuudella voidaan hakea tiettyä tunnusta.



Kuva 15. KeePass-tietokantanäkymä (KeePass 2021)

Kuten kuvassa 16 näkyy, jokaiseen merkintään voidaan tallentaa otsikko, käyttäjätunnus, salasana, URL-osoite, muistiinpanoja sekä asettaa tunnusten vanhentumisaika. Salasanaa syötettäessä ilmaistaan salasanan vahvuus bittteinä. Suurempi bittimäärä tarkoittaa turvallisempaa salasanaa.



Kuva 16. KeePass-tunnuksen lisääminen tietokantaan (KeePass 2021)

## 7.2 F-Secure ID PROTECTION

F-Secure on yksi maksullista salasanan hallintaohjelmaa tarjoavista tahoista. F-Secure ID PROTECTION sisältää salasanojen hallinnan lisäksi ympärivuorokautista monitorointia tietovuotojen varalta. Näin käyttäjille voidaan ilmoittaa reaaliajassa, mikäli heidän tietonsa ovat vuotaneet. Tietovuodon sattuessa ja sen kohdistuessa käyttäjän tietoihin tarjoaa F-Secure ohjeistusta, miten toimia, jotta tietovuoto ei muutu identiteettivarkaudeksi. (F-Secure 2021a.)

F-Secure ID PROTECTION tallentaa ja suojaa käyttäjän salasanoja, luottokorttinumeroita ja PIN-koodeja. Kaikki tiedot säilytetään salattuna ja ainoa

tapa päästä dataan käsiksi on pääsalasanalla. Data tallennetaan vain paikallisesti laitteelle, jossa F-Secure ID PROTECTION on käytössä. Näin dataa ei voida varastaa verkosta. (F-Secure 2021b.)

Data voidaan synkronoida useamman laitteen välillä, joissa on käytössä F-Secure ID PROTECTION. Kun tehdään muutoksia yhdellä laitteella, tallentuvat muutokset myös muille yhdistetyille laitteille. F-Secure suosittelee datan synkronointia ainakin toiselle laitteelle. Näin yhden laitteen menettäminen ei johda myös datan menettämiseen. Turvallisuussyistä ei pääsyä salasanoihin tarjota F-Securen palvelimien kautta. (F-Secure 2021b.)

F-Secure ID PROTECTION on saatavilla viiden tai kymmenen laitteen tilauksina. Näihin tilauksiin kuuluu sama määrä sähköpostitilien tietovuoto seurantaa. Tuettuja käyttöjärjestelmiä ovat Windows, macOS, Android ja iOS. (F-Secure 2021a.)

### **7.2.1 Turvallisuus**

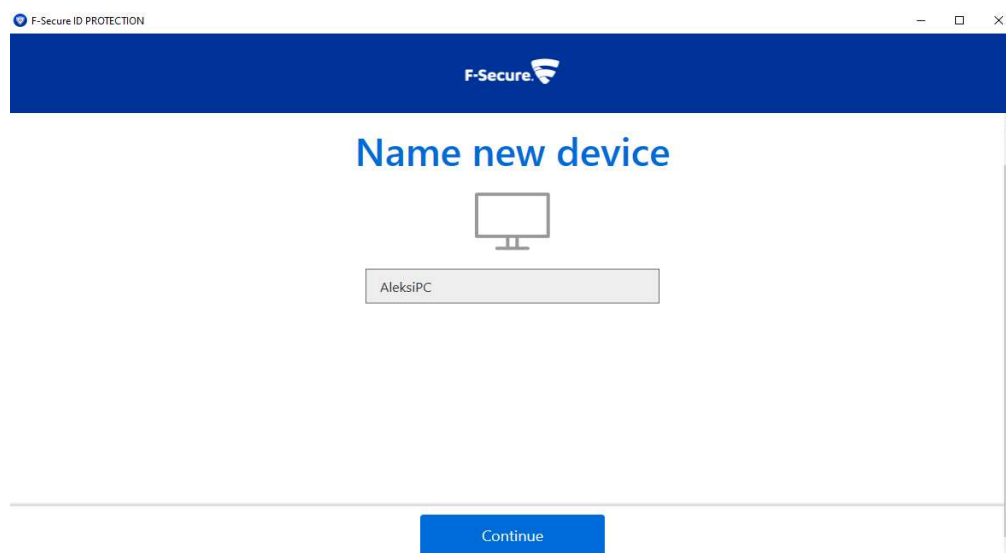
Tallennettu data salataan ja puretaan vain paikallisesti laitteella, johon F-Secure ID PROTECTION on asennettuna. Pääsalasanan syötettyä lisätään uusi salauskerros luomalla uusi salausavain PBKDF2-standardin mukaisesti, jolla datan salaus voidaan purkaa. PBKDF2 lisää pääsalasanaan suolauksen, eli satunnaista dataa, ja tästä saatu tuotos hajautetaan 20 000 kertaa käyttäen HMAC-SHA256-tiivistefunktiota. (F-Secure 2021b.)

Turvallisuussyistä pääsalasanaa ja salausavainta ei koskaan tallenneta ja luotu salausavain poistetaan, kun F-Secure ID PROTECTION suljetaan. Tästä syystä F-Securella ei ole mahdollisuutta palauttaa unohtunutta pääsalasanaa tai purkaa salattua dataa. (F-Secure 2021b.)

F-Secure suosittelee pääsalasanelle luotavaksi uniikin palautuskoodin. Tämä on ainoa tapa palauttaa pääsy tietokantaan pääsalasanan unohtuessa. Palautuskoodi on vahvasti salattu ja se voidaan purkaa vain yhdellä yhdistetyistä laitteista. Pääsykoodia suositellaan tallennettavaksi kuvan muodossa tai paperille tulostettuna. (F-Secure 2021b.)

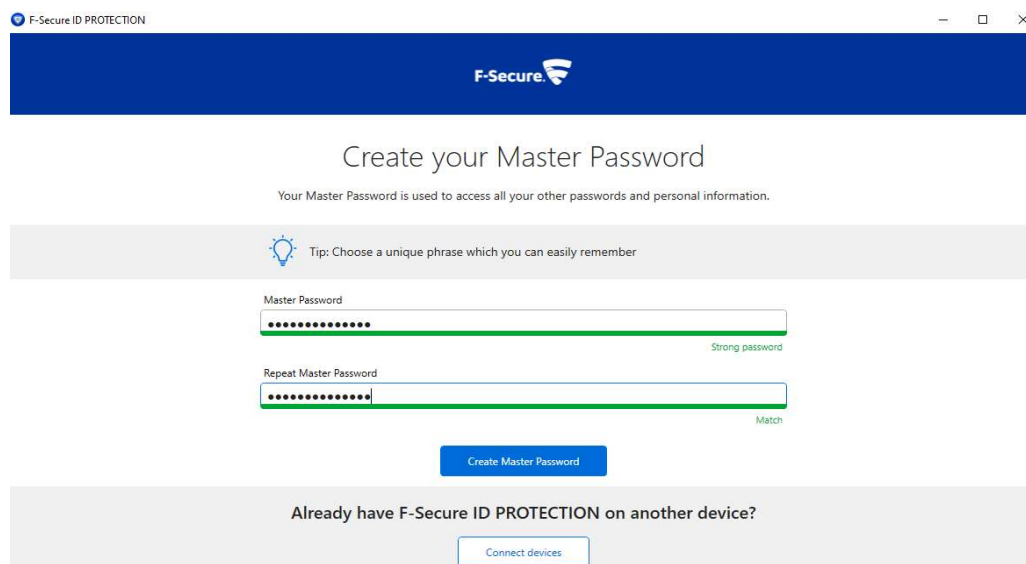
## 7.2.2 Käyttö

Onnistuneen tilauksen jälkeen asennetaan F-Secure ID PROTECTION halutulle laitteelle. Android- ja iOS-versiot ovat saatavilla Google Play- ja AppStore-sovelluskaupoista. Asennuksen yhteydessä pyydetään kyseinen laite nimeämään kuvan 17 mukaan.



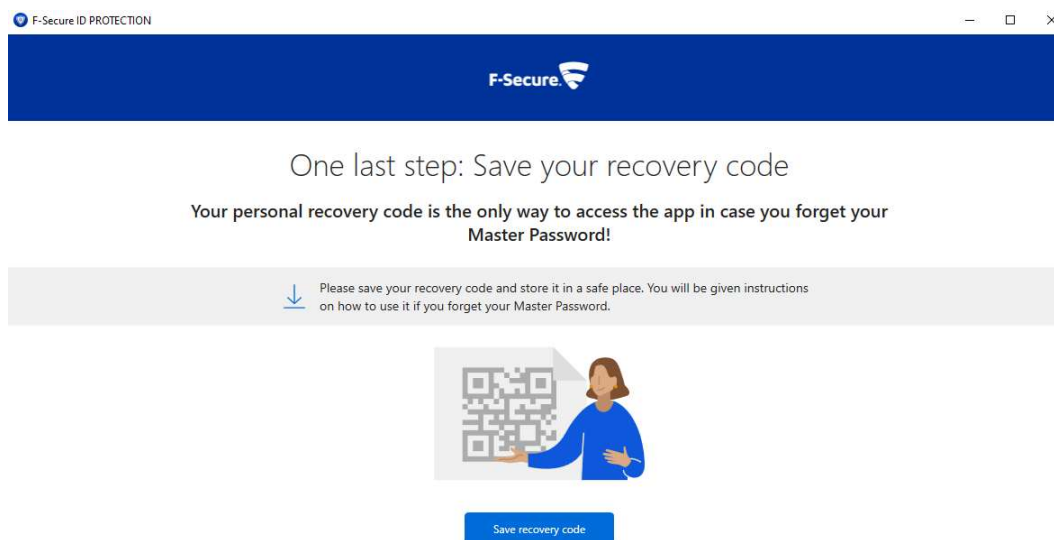
Kuva 17. ID PROTECTION laitteen nimeäminen (F-Secure 2021)

Tämän jälkeen käyttäjällä on kaksi vaihtoehtoa. Ensimmäisellä kerralla käyttäjä luo itselleen pääsalasanat palveluun, mikäli ID PROTECTION on jo käytössä, voidaan uusi laite synkronoida jo olemassa oleviin laitteisiin. Pääsalasanaa luotaessa ID PROTECTION kertoo kuvassa 18 salasanan vahvuuden ja muistuttaa, että salasanan tulisi olla uniikki ja helposti muistettava.



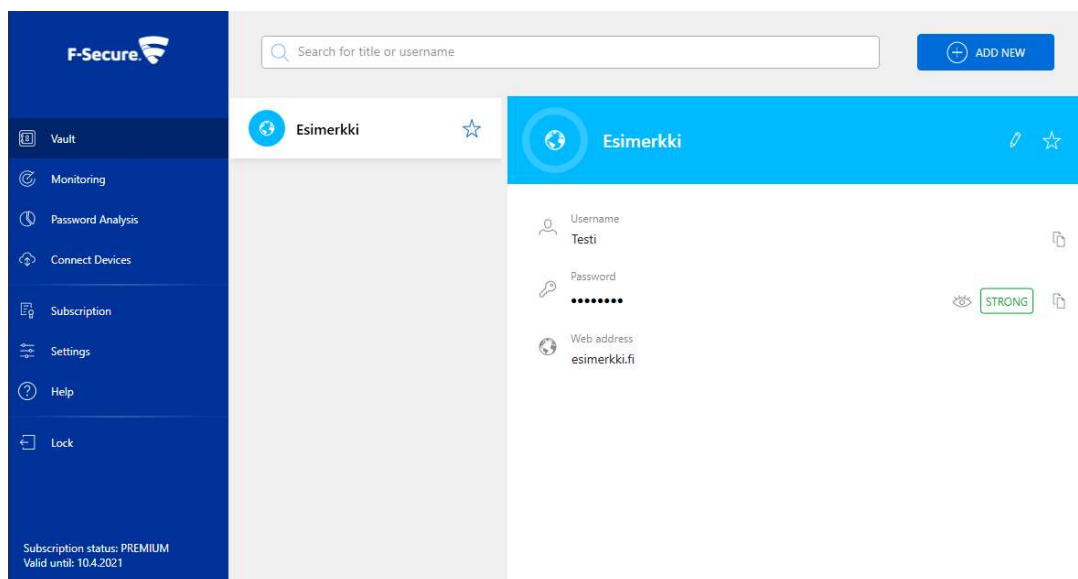
Kuva 18. ID PROTECTION pääsalasanan luominen (F-Secure 2021)

Ainoa tapa palauttaa tili käyttöön salasanan unohtamisen yhteydessä on palautuskoodi. ID PROTECTION ohjeistaa kuvassa 19 tallentamaan palautuskoodin. Palautuskoodin käyttö varten ID PROTECTION antaa ohjeistuksen pääsalasanan unohtumisen yhteydessä.



Kuva 19. ID PROTECTION palautuskoodin tallentaminen (F-Secure 2021)

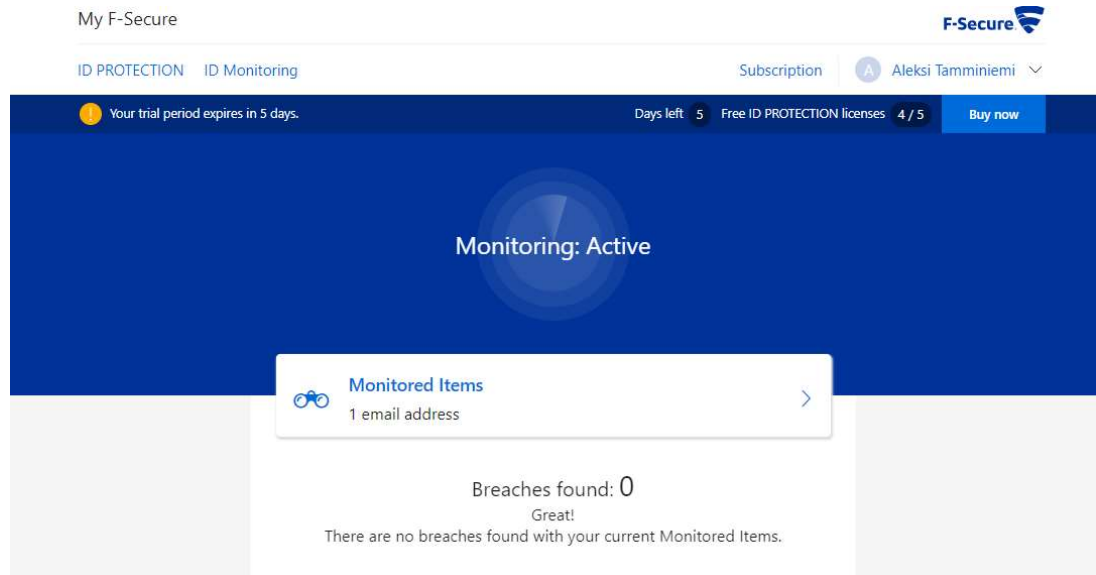
Tallennetut tunnukset näkyvät kuvan 20 mukaisesti ID PROTECTIONin Vault-välilehdellä. Täältä tunnuksia voi lisätä, poistaa tai muokata. Tunnuksille voi tallentaa verkko-osoitteen, jolloin ID PROTECTION täyttää kyseisen verkkosivun kirjautumispyynnön yhteydessä oikeat tunnukset automaattisesti, kun Google Chrome- tai Mozilla Firefox -laajennus on asennettuna.



Kuva 20. ID PROTECTION Vault näkymä (F-Secure 2021)

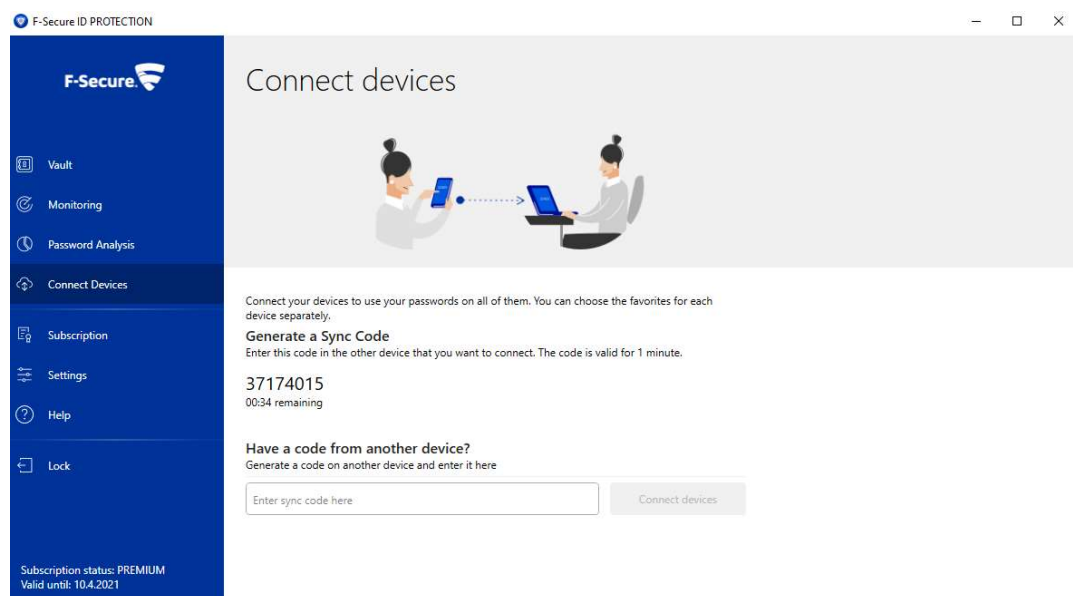


Monitoring -välilehdeltä sovellus ohjaa My F-Secure-verkkosivulle, josta voidaan ottaa käyttöön sähköpostiosoitteen valvonta tietovuotojen varalta. Kuvassa 21 on esimerkki aktiivisesta seurannasta ja sähköpostiosoitteisiin kohdistuneista tietovuodoista.



Kuva 21. ID Monitoring näkymä (F-Secure 2021)

Connect Devices -välilehdeltä voidaan synkronoida kahden laitteen ID PROTECTION sovellukset. Laitteiden yhdistäminen tapahtuu kuvan 22 mukaisesti synkronointikoodilla. Laitteiden ollessa synkronoituina keskenään päivittyvät toisella laitteella tehdyt muutokset automaattisesti myös muille laitteille.



Kuva 22. ID PROTECTION, laitteiden synkronointi (F-Secure 2021)

### 7.3 Riskit

Salasanan hallintaohjelmat parantavat käyttäjän turvallisuutta helpottamalla uniikkien salasanojen käyttöä eri palveluissa. Ne mahdollistavat myös turvallisempien salasanojen käytön, kun niiden muistamisen vastuu siirretään ihmiseltä ohjelmalle.

Näiden hyötyjen lisäksi nousee salasanan hallintaohjelma käytöstä esille muutamia riskejä. Kuten kaikissa muissa ohjelmissa, voi salasanan hallintaohjelmissa ilmaantua haavoittuvuuksia. Kaikkien salasanojen ja tunnusten ollessa tallennettuna yhteen paikkaan ovat ne houkuttelevia kohteita hyökkäyksille. Onnistunut hyökkäys mahdollistaa pääsyn kaikkiin niihin palveluihin, joiden salasanat ovat tallennettuna salasanan hallintaohjelman tietokantaan. (NCSC 2018.)

Tämä luvun perusteella voidaan päätellä, että pääsalasana on tärkeässä roolissa salasanan hallintaohjelmien käytössä. Pääsalasanan unohtaminen voi pahimmassa tapauksessa johtaa koko salasana tietokannan menettämiseen. Pääsalasana voi olla myös houkutteleva kohde tietojenkalastelu -yrityksissä.

## 8 YHTEENVETO

Monivaiheinen tunnistautuminen on suurelle osalle jo osa arkea työelämän kautta. Yrityksien panostaessa tietoturvaansa on myös monivaiheisen tunnistautuminen yleistynyt. Kaikki eivät kuitenkaan ole vielä omaksuneet sitä osaksi yksityistä tietoturvallisuuttaan. Tähän voi olla useita syitä, mutta pääsyinä pidetään ylimääräisenä koettua vaivaa tai se, etteivät monivaiheisen tunnistautumisen hyödyt ole selkeät.

Tämän työn tarkoituksena oli tuoda ilmi monivaiheisen tunnistautumisen hyötyjä ja madaltaa sen käyttöönoton kynnystä osana yksityisen tietoturvaa. Näin työlle muodostui tutkimuskysymys:

Miten yleisimmät monivaiheiset tunnistautumismenetelmät otetaan käyttöön ja mitkä ovat niiden hyödyt?

Tässä työssä käsiteltiin monivaiheinen tunnistautuminen ja siihen liittyvät tunnistetyypit. Työtä tehdessä huomattiin, että kaikille käsitellyille tunnistautumismenetelmille on olemassa jo palvelun tarjoajan dokumentaatio. Näiden dokumentaatioiden selkeys ja käytettävyys oli kuitenkin vaihtelevaa. Useassa tapauksessa käyttäjällä täytyy olla jo pohjatietoa menetelmän toimintaperiaatteesta käyttöönoton yhteydessä.

Eri tunnistetyyppien vahvuudet ja heikkoudet analysoitiin. Näiden perusteella voidaan valikoida kullekin sopiva tunnistautumismenetelmä. Läpi käydyistä monivaiheisen tunnistautumisen palveluista kirjoitettiin käyttö- ja käyttöönottopastus. Tarkka ja helposti luettava ohjeistus laskee käyttöönoton kynnystä. Lisäksi tuotettiin työstä erilleen jaettavaksi tarkoitettu infograafi monivaiheisesta tunnistautumisesta (ks. liite 1).

Koska työssä käsitellään monivaiheista tunnistautumista yksityisen henkilön näkökulmasta, koettiin sitä tehdessä hyödylliseksi käsitellä myös salasanan hallintohjelmia niiden ollessa osa yksityisen tietoturvaa.

Salasanan hallintaohjelmat helpottavat uniikkien salasanojen käyttöä eri palveluissa. Tämä nostaa usean salasanan muistamisen taakan pois ihmiseltä ja siirtää sen hallintaohjelmalle. Tämä tuo mukanaan riskejä, mutta niiden tuomat hyödyt koetaan riskien arvoisiksi. Salasanan hallintaohjelmia tarjoaa useampi eri yritys, mutta tähän työhön valikoitiin kaksi niiden vertaisarvioinnin mahdollistamiseksi. KeePass on maksuton avoimen lähdekoodin hallintaohjelma, kun taas F-Secure ID PROTECTION on maksullinen suljetun lähdekoodin hallintaohjelma. Näistä hallintaohjelmista tehtiin käyttö- ja käyttöönottopastus sekä analysoitiin salasanan hallintaohjelmien riskejä.

## **8.1 Pohdinta**

Monivaiheinen tunnistautuminen on tulevaisuudessa lähes välttämätöntä. Sen tarjoamia hyötyjä tietoturvallisuuden kannalta ei voida sivuttaa. Teknologian kehittyessä tulee se parantamaan nykyisiä ja tarjoamaan uusia tunnistautumismenetelmiä. Nämä uudet menetelmät tulevat vähentämään ihmiseltä tarvittavaa vuorovaikutusta, kun ihmisiä voidaan yksilöidä eri tunnisteilla aina tar-  
kemmin.

Yleisesti monivaiheinen tunnistautuminen ymmärretään tällä hetkellä kaksivaiheisena tunnistautumisena. Tunnistautumistapojen kehittyessä ja uusien saapuessa laajaan käyttöön tullaan kuitenkin puhumaan aidosti monivaiheisesta tunnistautumisesta. Kun ihmisen vuorovaikutus tunnistautumismenetelmien kanssa saadaan laskettua tarpeeksi matalalle, voidaan ihminen tunnistaa vahvemmin ja vaivattomammin usealla eri tavalla. Tämä tulee parantamaan tietoturvallisuutta ja käyttäjäystävällisyyttä huomattavasti.

Tällainen ihmisten tunnistaminen tulee kuitenkin herättämään huolia ihmisten yksityisyyden suojasta. Kaikkien tunnisteiden pitää kuitenkin olla tallennettu johonkin, jotta tunnistautuminen onnistuu. Tämä tekee näitä tietoja säilyttävistä yrityksistä houkuttelevia kohteita kyberhyökkäyksille.

Työssä saavutettiin asetetut tavoitteet. Työssä käsiteltiin muutama monivaiheisen tunnistautumisen menetelmä. Näiden pohjalta saadaan kattava ymmärrys monivaiheisen tunnistautumisen toiminnasta. Tavoitteiden ulkopuolelta koettiin edukkaaksi käsitellä myös salasanan hallintaohjelmia. Kahden käsitellyn hallintaohjelman pohjalta saadaan hyvä ymmärrys hallintaohjelmien toiminnasta.

## **8.2 Jatkokehitys**

Tässä työssä käsiteltiin tunnistetyppejä erittäin kansanomaisesti. Ihmisen yksilöiviä tekijöitä on monia, ja näiden pohjalta voidaan luoda uusi tunnisteita. Näistä esimerkkinä on ihmisen kirjoitustavan tunnistava tekoälypohjainen tunnistautuminen. Tällaista tunnistautumispalvelua tarjoaa muun muassa TypingDNA.

Vastaavia vähemmän käytössä olevia tunnisteita on varmasti jo monia. Näiden kehittyessä ja yleistyessä saadaan niistä myös enemmän tietoa. Opinnäytetyö näistä uudemmissa ja monimutkikkaammista tunnistautumistavoista olisi hyvä jatkumo tutkimukselle.

## LÄHTEET

AWS. 2021. Using multi-factor authentication (MFA) in AWS. WWW-dokumentti. Saatavissa: [https://docs.aws.amazon.com/IAM/latest/User-Guide/id\\_credentials\\_mfa.html](https://docs.aws.amazon.com/IAM/latest/User-Guide/id_credentials_mfa.html) [viitattu 1.2.2021].

Cisco. 2020. What Is Multi-Factor Authentication? WWW-dokumentti. Saatavissa: <https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html> [viitattu 26.1.2021].

DNA. 2020. DNA Mobiilivarmenne -tunnistusperiaatteet. DNA Oy. WWW-dokumentti. Saatavissa: [https://www.dna.fi/documents/753910/853444/Mobiilivarmenne\\_tunnistusperiaatteet.pdf/78effbdc-51b5-b241-a43b-01b67a65740a](https://www.dna.fi/documents/753910/853444/Mobiilivarmenne_tunnistusperiaatteet.pdf/78effbdc-51b5-b241-a43b-01b67a65740a) [viitattu 29.11.2020].

Elisa. 2014. Varmennuskäytäntö. Elisa Oyj. WWW-dokumentti. Saatavissa: [https://elisa.fi/attachment/content/ELISA-Oyj-Varmennuskaytanto-Asiointivarmenne-1\\_2.pdf](https://elisa.fi/attachment/content/ELISA-Oyj-Varmennuskaytanto-Asiointivarmenne-1_2.pdf) [viitattu 26.1.2021].

Elisa. 2020. Tunnistusperiaatteet – Elisa Mobiilivarmenne. Elisa Oyj. WWW-dokumentti. Saatavissa: <https://elisa.fi/attachment/content/Tunnistusperiaatteet-Mobiilivarmenne.pdf> [viitattu 29.11.2020].

F-Secure. 2021a. F-Secure ID PROTECTION. WWW-dokumentti. Saatavissa: <https://www.f-secure.com/en/home/products/id-protection> [viitattu 4.4.2021].

F-Secure. 2021b. About ID PROTECTION. WWW-dokumentti. Saatavissa: [https://help.f-secure.com/product.html#home/id-protection/latest/en/concept\\_8AB7E2314E8B4D4EB633D1A13A683C31-id-protection-latest-en](https://help.f-secure.com/product.html#home/id-protection/latest/en/concept_8AB7E2314E8B4D4EB633D1A13A683C31-id-protection-latest-en) [viitattu 4.4.2021].

Google. 2021. Tilin suojaaminen kaksivaiheisella vahvistuksella. WWW-dokumentti. Saatavissa: <https://support.google.com/accounts/answer/185839?co=GENIE.Platform%3DDesktop&hl=fi> [viitattu 17.3.2021].

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 16. painos. Helsinki: Tammi.

Jyväskylän yliopisto. 2015. Määrällinen tutkimus. WWW-dokumentti. Saatavissa: <https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/maarallinen-tutkimus> [viitattu 15.3.2021].

KeePass. 2021. KeePass Password Safe. WWW-dokumentti. Saatavissa: <https://keepass.info/> [viitattu 25.3.2021].

Kyberturvallisuuskeskus. 2021. Salasanat haltuun - Kuka käyttää tiliäsi? WWW-dokumentti. Saatavissa: <https://www.kyberturvallisuuskeskus.fi/fi/ajan-kohtaista/ohjeet-ja-oppaat/salasanat-haltuun> [viitattu 26.1.2021].

Lapin ammattikorkeakoulu. 2021. Opinnäytetyön toteuttaminen. WWW-dokumentti. Saatavissa: <https://www.lapinamk.fi/fi/Opiskelijalle/Opinto-opas,-AMK-tutkinto/Opinnaytetyoohje/Opinnaytetyon-toteuttaminen> [viitattu 15.3.2021].

Metsämuuronen, J. 2006. Laadullisen tutkimuksen käsikirja. Jyväskylä: International Methelp Ky.

Microsoft. 2019. One simple action you can take to prevent 99.9 percent of attacks on your accounts. WWW-dokumentti. Saatavissa: <https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/> [viitattu 26.1.2021].

Microsoft. 2021a. How to use the Microsoft Authenticator app. WWW-dokumentti. Saatavissa: <https://support.microsoft.com/en-us/account-billing/how-to-use-the-microsoft-authenticator-app-9783c865-0308-42fb-a519-8cf666fe0acc> [viitattu 6.3.2021].

Microsoft. 2021b. How to use two-step verification with your Microsoft account. WWW-dokumentti. Saatavissa: <https://support.microsoft.com/en-us/account-billing/how-to-use-two-step-verification-with-your-microsoft-account-c7910146-672f-01e9-50a0-93b4585e7eb4> [viitattu 6.3.2021].

Microsoft. 2021c. Turning two-step verification on or off for your Microsoft account. WWW-dokumentti. Saatavissa: <https://support.microsoft.com/en-us/account-billing/turning-two-step-verification-on-or-off-for-your-microsoft-account-b1a56fc2-caf3-a5a1-f7e3-4309e99987ca> [viitattu 6.3.2021].

Microsoft. 2021d. What authentication and verification methods are available in Azure Active Directory? WWW-dokumentti. Saatavissa: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods> [viitattu 1.2.2021].

Milka, G. 2018. Anatomy of Account Takeover. Google. USENIX Enigma 2018. Conference in Santa Clara, California 16-18.1.2018. Youtube. Videoleike. Julkaistu 21.2.2018 Saatavissa: <https://www.youtube.com/watch?v=W2a4fRlshI> [viitattu 5.11.2020].

Mobiilivarmenne. 2020a. DNA:n asiakas: näin rekisteröit Mobiilivarmenteen käyttösi. WWW-dokumentti. Saatavissa: <https://mobiilivarmenne.fi/2017/10/02/dnan-asiakas-nain-rekisteroit-mobiilivarmenteen-kayttoosi/> [viitattu 14.12.2020].

Mobiilivarmenne. 2020b. Elisan asiakas: näin aktivoit Mobiilivarmenteen käyttösi. WWW-dokumentti. Saatavissa: <https://mobiilivarmenne.fi/2017/10/02/elisan-asiakas-nain-aktivoit-mobiilivarmenteen-kayttoosi/> [viitattu 14.12.2020].

Mobiilivarmenne. 2020c. Mobiilivarmenne on helppo ja turvallinen tapa kirjautua verkkopalveluihin matkapuhelimellasi. WWW-dokumentti. Saatavissa: <https://mobiilivarmenne.fi/> [viitattu 29.11.2020].

Mobiilivarmenne. 2020d. Telian asiakas: näin aktivoit Mobiilivarmenteen käyttösi. WWW-dokumentti. Saatavissa: <https://mobiilivarmenne.fi/2017/10/02/telian-asiakas-nain-aktivoit-mobiilivarmenteen-kayttoosi/> [viitattu 14.12.2020].

National Cyber Security Centre. 2018. Password administration for system owners. WWW-dokumentti. Saatavissa: <https://www.ncsc.gov.uk/collection/passwords/password-manager-buyers-guide> [viitattu 7.4.2021].

Telia. 2020. Mobiilivarmenne. Telia Finland Oy. WWW-dokumentti. Saatavissa: <https://www.telia.fi/asiakastuki/palvelut/mobiilivarmenne> [viitattu 29.11.2020].

## KUVALUETTELO

Kuva 1. DNA Mobiilivarmenne puhelinnumero. Mobiilivarmenne 2020a

Kuva 2. DNA Mobiilivarmenne tarkistus. Mobiilivarmenne 2020a

Kuva 3. DNA Mobiilivarmenne tunnusluvunluonti. Mobiilivarmenne 2020a

Kuva 4. Elisa Mobiilivarmenne liittymän kelpoisuus. Mobiilivarmenne 2020b

Kuva 5. Elisa Mobiilivarmenne yhteystiedot. Mobiilivarmenne 2020b

Kuva 6. Elisa Mobiilivarmenne tunnusluvut. Mobiilivarmenne 2020b

Kuva 7. Telia Mobiilivarmenne puhelinnumero. Mobiilivarmenne 2020d

Kuva 8. Telia Mobiilivarmenne kontrollinumero. Mobiilivarmenne 2020d

Kuva 9. Google kaksivaiheinen tunnistautuminen. Google 2021

Kuva 10. Google kaksivaiheisen tunnistautumisen vaihtoehtoja. Google 2021

Kuva 11. Microsoft turvallisuusasetukset kaksivaiheinentunnistautuminen. Google 2021

Kuva 12. Microsoft kaksivaiheinen tunnistautuminen otettu käyttöön. Microsoft 2021

Kuva 13. Microsoft kaksivaiheinen tunnistautuminen käytössä. Microsoft 2021

Kuva 14. KeePass tietokannan avaaminen pääsalasanalla. KeePass 2021

Kuva 15. KeePass-tietokantanäkymä. KeePass 2021

Kuva 16. KeePass-tunnuksen lisääminen tietokantaan. KeePass 2021

Kuva 17. ID PROTECTION laitteen nimeäminen. F-Secure 2021

Kuva 18. ID PROTECTION pääsalasanan luominen. F-Secure 2021

Kuva 19. ID PROTECTION palautuskoodin tallentaminen. F-Secure 2021

Kuva 20. ID PROTECTION Vault näkymä. F-Secure 2021

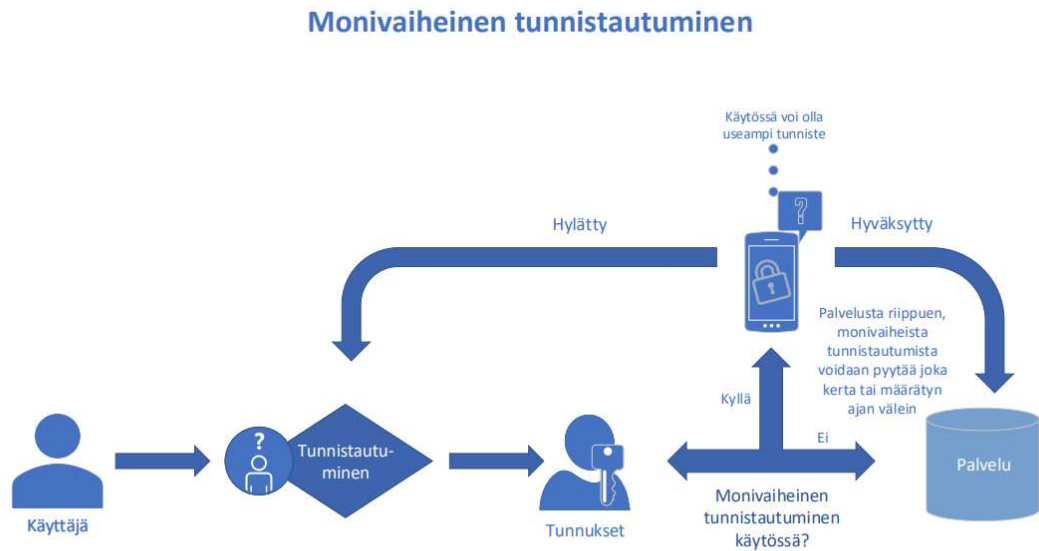
Kuva 21. ID Monitoring näkymä. F-Secure 2021

Kuva 22. ID PROTECTION, laitteiden synkronointi. F-Secure 2021



## LIITTEET

## Liite 1. Infograafi Monivaiheinen tunnistautuminen



**Miten monivaiheinen tunnistautuminen suojaa käyttäjän palveluita tietovuodon yhteydessä?**

