
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

ONNI VILJANEN

# Salasanojen hallintasovellukset

TIETOJENKÄSITTELYN KOULUTUSOHJELMA
2023

Tekijä
Viljanen, Onni

Julkaisun laji
Opinnäytetyö, AMK

Päivämäärä
09/2023

Sivumäärä
28

Julkaisun kieli
Suomi

Julkaisun nimi
**Salasanojen hallintasovellukset**

Tutkinto-ohjelma
Tietojenkäsittelyn koulutusohjelma

Tiivistelmä

Tässä opinnäytetyössä tutustuttiin erilaisiin salasanojen hallintasovellustyyppeihin ja niiden käyttöön. Työn tarkoituksena oli antaa lukijalle käsitys siitä, miten ja miksi hallintasovelluksia tulisi käyttää.

Työssä käytiin läpi yleisiä asioita salasanoista, salasanojen historiaa, vaihtoehtoisia todennusmenetelmiä ja niiden ongelmia, ja lopuksi salasanojen hallintasovelluksia ja niiden ominaisuuksia. Ominaisuuksia vertailtiin keskenään, ja tarkoituksena oli löytää yleisesti paras hallintasovellustyyppi.

Työ toteutettiin englanninkielisen materiaalin sekä oman tiedon ja pohdinnan avulla.

Asiasanat
Salasanojen hallintasovellukset, tietoturva

Author
Viljanen, Onni

Type of Publication
Bachelor's thesis

Date
09/2023

Number of pages
28

Language of publication:
Finnish

Title of publication
**Password managers**

Degree program
Business Information Technology

Abstract

This thesis focused on exploring different types of password managers and how to use them. The purpose was to give the reader an idea of how and why password managers should be used.

The thesis examined common things about passwords and their history, alternate methods of authentication and their problems, and lastly, password managers and their features. The features were compared together, and the purpose was to find the best type of password manager in a general sense.

The work was carried out using material in English with the help of my own knowledge and pondering.

Key words
Password managers, security

# SISÄLLYS

# 1 JOHDANTO

Teknologian kehittyessä myös tietoturvan tarve kehittyy. Nykypäivänä huomattava osa elämästä tapahtuu verkossa; sosiaalinen media, kaupankäynti, työt sekä muu sähköinen kommunikointi. Tällöin salasanojen pitäminen turvassa on suuressa roolissa niin yksityishenkilöille kuin yrityksille. Salasanojen tietoturva ei ole pelkästään tärkeää, vaan se on välttämätöntä. Vaikka perinteinen salasana on kaikista suosituin tapa varmentaa käyttäjä, salasanan käyttöön liittyy kuitenkin useita riskejä ja tietoturvaongelmia. Yksi tietoturvan tärkeimmistä säännöistä on, että samaa salasanaa ei tule käyttää eri palveluissa, eikä salasanoja kannata kirjoittaa muistiin fyysisesti tai virtuaalisesti. Salasanoista tulee myös tehdä tarpeeksi monimutkaisia, jotta ne olisivat mahdollisimman turvallisia. Salasanojen erilaisten turvallisuusvaatimusten johdosta moni käyttäjä päätyy unohtamaan salasanansa. Salasanojen hallintaan täytyy siis olla käyttäjäystävällisempi keino kuin useamman monimutkaisen salasanan muistaminen ulkoa.

Tässä opinnäytetyössä käydään ensin läpi yleisiä asioita salasanoihin liittyen, salasanojen historiaa sekä salasanojen riskejä ja ongelmia. Tästä siirrytään vaihtoehtoisiin todennusmenetelmiin, joita voidaan käyttää salasanojen sijaan. Tämän jälkeen käsitellään pääaihetta, eli salasanojen hallintasovelluksia. Salasanojen hallintasovellustyyppejä vertaillaan keskenään. Tarkoituksena on selvittää, miten eri hallintasovellustyyppien ominaisuudet eroavat toisistaan, ja mikä hallintasovellustyyppi on yleisesti paras vaihtoehto.

# 2 SALASANOJEN KÄYTTÖ

## 2.1 Yleistä

Salasana on merkkijono, jota käytetään käyttäjän tunnistamiseen erilaisissa laitteissa, sovelluksissa sekä verkkosivuilla. Tyypillisesti salasanaa käytetään yhdessä käyttäjätunnuksen kanssa, ja ainoastaan käyttäjän on tarkoitus tietää salasanansa. Salasanat voivat olla eripituisia, ja niissä voi olla useampia merkkejä. Salasanan turvallisuus on myös tärkeää. Turvallisen salasanan luonnissa tulee pyrkiä käyttämään useampaa merkkiä, kuten pieniä sekä isoja kirjaimia, numeroita sekä erikoismerkkejä. Nykyään useat palvelut käyttävät käyttäjätunnuksen luonnin yhteydessä salasanan vahvuustarkastusta, jolloin helposti arvattavia salasanoja on mahdotonta asettaa salasanaksi. Esimerkiksi merkkijonot “123456” sekä “qwerty” eivät yleensä kelpaa salasanaksi, sillä ne ovat todella yleisiä ja helposti arvattavia. (Rouse 2017a.) Salasana on kaikista suosituin tapa todentaa käyttäjä; sitä vaaditaan muun muassa tietokoneelle kirjautumiseen, puhelimen avaamiseen, verkkoon liittymiseen sekä itsensä varmentamiseen lähes kaikissa palveluissa.

## 2.2 Historiaa

Historian ensimmäinen salasanaa vaativa kirjautuminen tietokoneelle kehitettiin vuonna 1961 Massachusettsissa. Samana vuonna tapahtui myös ensimmäinen salasanoihin liittyvä murto, jossa tutkija tulosti käyttäjien salasanoja ja jakoi niitä muille käyttäjille. Vuosien varrella tapahtunut teknologian kehitys johti myös yhä useamman salasanan murtamiseen eri keinoin, minkä johdosta vuonna 1979 amerikkalainen virasto NBS (National Bureau of Standards) kehitti DES-salausmenetelmän (Data Encryption Standard). DES toimi standardina lähes 20 vuotta, mutta kuten saattaa arvata, teknologian vauhdikkaan kehittymisen johdosta myös salausmenetelmiä piti vahvistaa. Vuonna 1988 pahamaineinen haittaohjelma Morris Worm teki kiusaa tuhansille tietokoneille muun muassa arvaamalla heikkoja salasanoja. Tämä johti siihen, että vuonna 1997 kaksi tiedemiestä loi AES-salausmenetelmän (Advanced Encryption Standard), josta tuli nopeasti suosittu. (Foster 2020.)

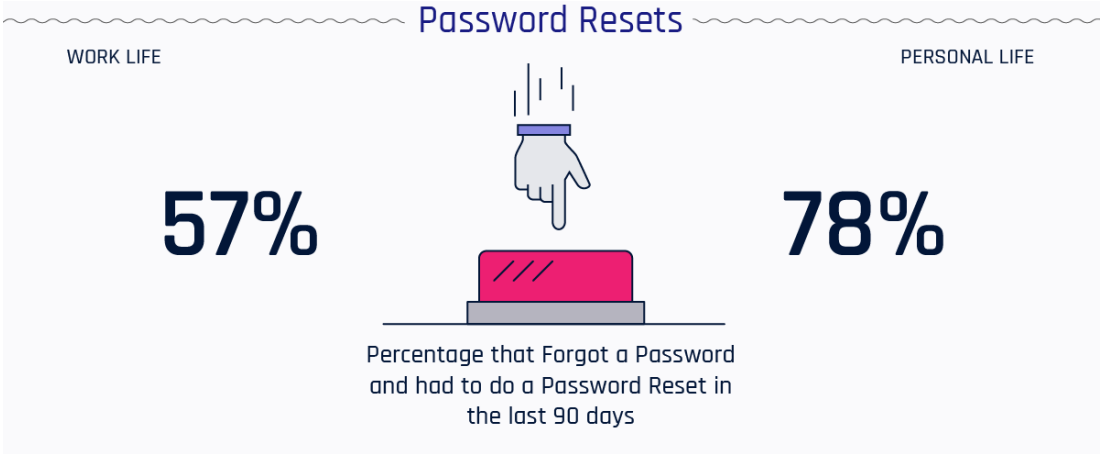
## 2.3 Riskit ja ongelmat

Vaikka yhä useampi palvelu edellyttää turvallisen salasanan asettamista, liittyy siihenkin useita riskejä ja ongelmia. Mitä monimutkaisempi salasana on, sitä vaikeampi se on muistaa. Tämän lisäksi samaa salasanaa ei suositella käyttämään useassa eri palvelussa, jolloin muistettavien salasanojen määrä kasvaa huomattavasti. Muistamisen auttamiseksi osa käyttäjistä kirjoittaa salasanansa muistiin paperille tai tietokoneen tekstitiedostoon; mikä voisi mennä vikaan?

### 2.3.1 Fyysiset uhat

Salasanojen kirjoittaminen muistiin on siinä mielessä huono vaihtoehto, että käytännössä kuka vain voi päästä niihin käsiksi. Esimerkiksi käyttäjän luona kylässä oleva tuttu saattaa löytää käyttäjän kirjoittaman paperilapun, johon on kirjoitettu salasanojen lisäksi mahdollisesti myös käyttäjätunnukset ja palveluiden nimet, joihin tunnuksilla pääsee kirjautumaan.

Salasanojen pitäminen muistissa omassa päässä voi olla myös haastavaa. Tietoturvayritys HYPR:n tekemän tuoreen tutkimuksen mukaan 78% ihmisistä on unohtanut ja joutunut resetoimaan yksityiselämän salasanansa viimeisten 90 päivän aikana. Vastaavasti 57% ihmisistä on unohtanut ja resetoinut työelämän salasanansa viimeisen 90 päivän aikana (kuva 1). Samassa tutkimuksessa todettiin, että 37%:lla on yli kaksikymmentä henkilökohtaisen elämän salasanaa, ja 19%:lla on työelämässään yli kymmenen salasanaa. (Castro 2019.)




Kuva 1. Käyttäjät, jotka ovat unohtaneet salasanansa viimeisen 90 päivän aikana ja joutuneet resetoimaan sen (Castro 2019)

### 2.3.2 Kyberuhat

Yksi varteenotettava ongelma on näppäilytallennin (keylogger). Vaikka monimutkaiset salasanat olisivat muistissa vain käyttäjän omassa päässä, niin näppäilytallennin mahdollistaa salasanojen sieppaamisen helposti. Käytännössä kaikki, mitä käyttäjä tietokoneellaan kirjoittaa, voi päätyä näppäilytallentimen takia ulkopuolisen käsiin.

Myös brute-force -hyökkäykset ovat mahdollisia, ja näitä hyökkäyksiä ei aina voi estää edes vahvalla salasanalla. Brute-force -hyökkäyksen perustana toimii ihminen tai robotti, joka yrittää arvata salasanaa useamman kerran. Useimmiten kyseisessä hyökkäyksessä kokeillaan ensisijaisesti yksinkertaisia ja lyhyehköjä salasanoja, jotka voivat löytyä esimerkiksi sanakirjoista tai kirjallisuudesta. Salasanamurtojen yhteydessä löytyneet salasanat vuodetaan yhdessä tai useammassa salasanoja sisältävässä tiedostossa (password dump) nettiin kaikkien nähtäville. Tälläkin hetkellä internetin syövereistä löytyy miljoonia potentiaalisesti käytössä olevia salasanoja. Vuodetuista salasanalistoista voi hahmottaa kaavoja ihmisten salasanojen käytöstä, ja tätä tietoa on mahdollista käyttää sekä hyödyllisiin että haitallisiin tarkoituksiin. Myös kekseliäät salasanat voivat koitua avoimiksi, jos salasanojen kaavoista on tarpeeksi tietoa. Esimerkkejä kekseliäistä salasanoista ovat “qwerty678^&*” ja “P@ssw0rd”. Kun tämänlaisia kaavoja löydetään, tietokoneohjelma osaa lisätä kyseiset salasanat yleisten salasanojen listalle, jolloin näistäkin salasanoista tulee riskialttiita. (Mitchell 2015.)

Joidenkin palveluiden tietoturvaan kuuluu, että salasana täytyy vaihtaa tietyin väliajoin. Osa asiantuntijoista on sitä mieltä, että salasanojen pakollisesta vaihtamisesta tulisi luopua. Salasanan pakollinen vaihtaminen johtaa usein siihen, että vanhaan salasanaan tehdään pieni muutos, jolloin salasana pysyy käytännössä samana, mutta nyt vähemmän turvallisena. Amerikkalainen virasto NIST (entinen NBS) luopui pakollisista salasanojen vaihdoista vuonna 2016. (Armerding 2019.) Vuonna 2010 tehdyssä tutkimuksessa tutkittiin kymmentätuhatta entistä käyttäjätiliä, jotka kuuluivat erään korkeakoulun entisille oppilaille, opettajille sekä muulle henkilökunnalle. Tutkijat loivat algoritmin, joka yritti arvata käyttäjätilien vanhoja salasanoja. Kun algoritmi arvasi jopa yhden vanhan salasanan, se arvasi myös seuraavan salasanan alle viidellä yrityksellä 17%:ssa käyttäjätileistä. (Cranor 2016.) Tutkimuksesta käy ilmi, miten helposti vanhan salasanan avulla voi arvata käyttäjän uudet salasanat, mikäli salasanaan tekee aina vain pieniä muutoksia.

Mielestäni erityisen huolestuttavaa on sekä fyysisten että verkon kautta tapahtuvien tietomurtojen jatkuva lisääntyminen ja niiden estämisen hankaluus. Tietoturva ei ole kaikille itsestäänselvyys, ja varsinkin ikäihmisillä on taipumusta käyttää salasanoissaan muun muassa lapsenlapsen nimeä ja syntymävuotta, tai vaikkapa perheen lemmikkikoiran nimeä ja omaa syntymävuottaan.

# 3 MAHDOLLISUUDET

Perinteisen salasanan suosio ei välttämättä kestä enää kauaa, kun yhä useampi käyttäjä siirtyy ajan kuluessa turvallisempiin todennusmenetelmiin. Salasanoille onkin jo kehitetty monia vaihtoehtoja, jotka tarjoavat huomattavasti paremman tietoturvan ja käytettävyyden. Tunnetuimpia vaihtoehtoja ovat monivaiheinen todennus, erilaiset biometriset varmennusmenetelmät sekä salasanojen hallintasovellukset.

### 3.1 Monivaiheinen todennus

Useat yritykset ovat jo ottaneet monivaiheisen todennuksen (kuva 2) käyttöön: Käyttäjä linkittää puhelinnumeronsa palveluun. Tämän jälkeen käyttäjä kirjautuu normaalisti sisään käyttäjätunnuksella ja salasanalla, jonka jälkeen käyttäjä vastaanottaa puhelimeensa tekstiviestin. Tekstiviesti on useimmiten 6-8-numeroinen koodi. Koodi syötetään palveluun, jolloin palvelu tarkistaa koodin oikeellisuuden. Tämä metodi antaa paremman suojakerroksen, koska yleensä ainoastaan käyttäjällä itsellään on fyysinen pääsy puhelimeensa. Teoreettisesti monivaiheinen todennus on siis paljon turvallisempi kuin pelkkä salasana. (CyberAvengers 2019.) Tunnettu esimerkki monivaiheisesta todennuksesta on pankkiasioinnissa käytettävä avainlukulista, jossa pankin sivuille kirjauduttaessa sekä maksua suoritettaessa käyttäjää pyydetään syöttämään avainlukulistalta tiettyä avainta vastaava luku (Lacort 2016). Käyttäjän todentaminen on tärkeää erityisesti pankkiasioinnissa, sillä jos ulkopuolinen taho pääsee käyttäjän rahoihin käsiksi, seuraukset voivat olla katastrofaaliset.


Kuva 2. Monivaiheisen todennuksen eri vaiheet (Imperva n.d.)

### 3.2 Biometrinen varmennus

Biometrinen varmennus on turvaprosessi, joka perustuu käyttäjän ainutlaatuisiin biologisiin tuntomerkkeihin. Tällä varmennetaan, että käyttäjä on oikeasti käyttäjä itse. Biometrisiä varmennustapoja ovat muun muassa sormenjälkitunnistus, kasvojentunnistus sekä silmäskannaus. (Rouse 2014b.) Biometrisen varmennuksen suosio

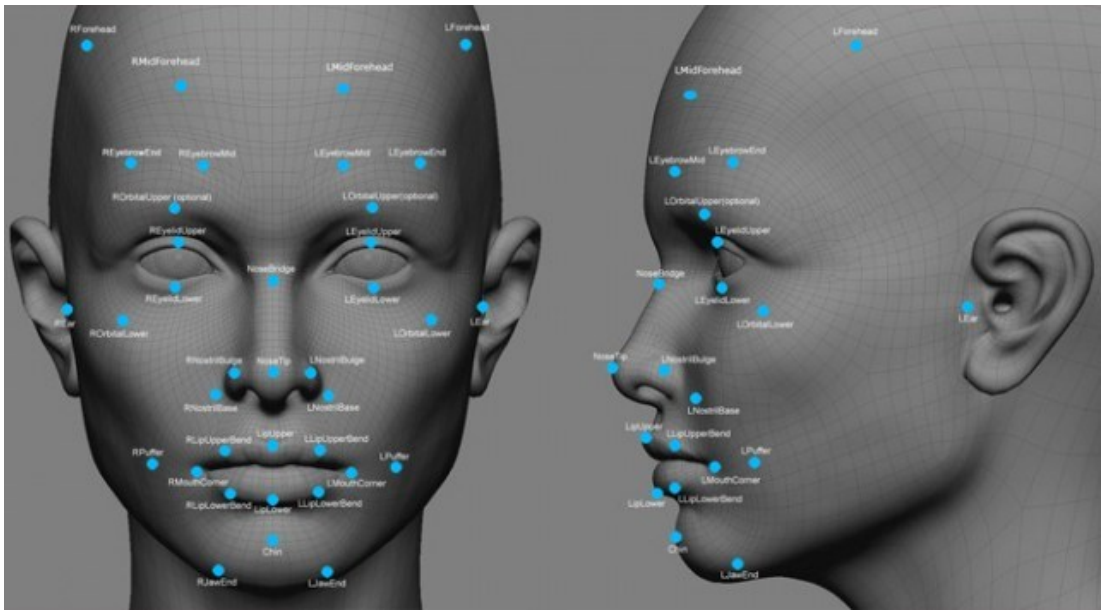
kasvaa vuosi vuodelta yhä enemmän sen tarjoaman helppokäyttöisyyden ja turvallisuuden vuoksi. Helppokäyttöisyys tulee esiin varsinkin sellaisessa tilanteessa, jossa käyttäjän pitäisi kirjoittaa kaksikymmentä merkkiä pitkä salasana. Biometrinen varmennus mahdollistaa sen, että käyttäjä voi yksinkertaisesti asettaa sormensa, silmänsä tai koko kasvonsa skannattavaksi pitkän salasanan kirjoittamisen sijaan.

### 3.2.1 Sormenjälkitunnistus

Sormenjälkitunnistuksen käyttö on lisääntynyt huomattavasti viime vuosina älypuhelimien johdosta. Vuonna 2013 julkaistu iPhone 5s -puhelin oli ensimmäinen sormenjälkiskannauksen omaava puhelin, ja nykypäivänä useimpien valmistajien puhelinmalleista löytyy jonkin asteen sormenjälkiskannaus. Skannaus toimii niin, että optinen lukija ottaa digitaalisen kuvan käyttäjän sormenjäljestä ja tallentaa sen. Tämän jälkeen käyttäjä voi aina todentaa itsensä asettamalla sormensa optiseen lukijaan. (Lacort 2016.)

### 3.2.2 Kasvojentunnistus

Kasvojentunnistuksen tarkoitus on tunnistaa käyttäjän kasvot teknologian kautta. Kasvojentunnistusjärjestelmä käyttää biometriaa ja algoritmeja käyttäjän tunnistamiseen (kuva 3). Vaikka algoritmit saattavat vaihdella eri järjestelmien välillä, perusvaiheet ovat samat: Käyttäjä toimittaa järjestelmään kuvan kasvoistaan. Järjestelmä lukee kasvojen mittasuhteet ja tunnusmerkit, jonka jälkeen ne tallennetaan tietokantaan. Avaintekijöitä ovat muun muassa silmien etäisyys toisistaan sekä välimatka otsasta leukaan. (Symanovich 2019.)




Kuva 3. Facebookin kasvojentunnistusohjelma DeepFace (Anthony 2019)

### 3.2.3 Verkkokalvoskannaus

Verkkokalvoskannaus on yksi tunnetuimmista mutta vähiten käytetyistä biometrisistä varmennustavoista. Verkkokalvoskannaus perustuu käyttäjän silmän verkkokalvosta otettuun kuvaan, joka otetaan infrapunavalon avulla käyttäjän katsoessa skanneriin. Verkkokalvon kuvan ottamisen jälkeen skannerin ohjelma yhdistää verkkokalvon ainutlaatuiset piirteet biometriseksi varmennusmenetelmäksi, jolloin käyttäjä voi käyttää silmäänsä tunnistautumiseen. Verkkokalvoskannaus on erittäin luotettava varmennustapa, sillä se on erittäin tarkka ja vaikeasti väärennettävä. Tämä johtuu siitä, että silmäskannauksessa käytettävät algoritmit vaativat verkkokalvosta korkealaatuisen ja selkeän kuvan. (King 2013.) Verkkokalvoskannausta ei tule sekoittaa värikalvoskannaukseen, jonka pääroolissa on silmän värikalvo. Esimerkiksi puhelimen silmäskannauksesta puhuttaessa kyseessä on värikalvoskannaus, sillä värikalvoskannaus toteutetaan kameran avulla, ja toistaiseksi missään puhelimessa ei ole vielä verkkokalvoskanneria.

### 3.2.4 Biometrisen varmennuksen ongelmat

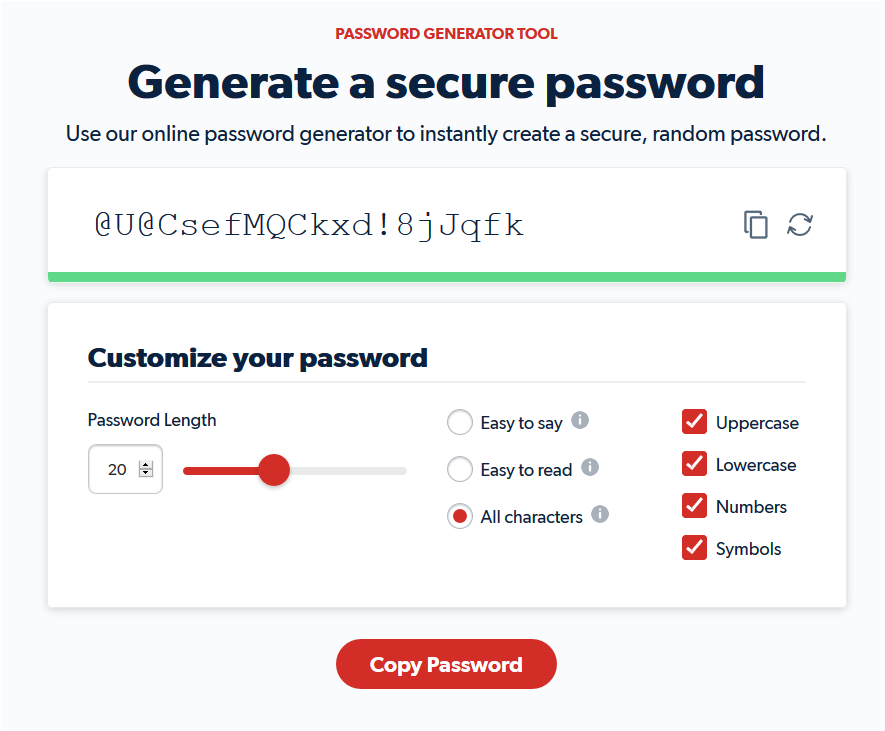
Vaikka biometrinen varmennus on pääsääntöisesti luotettava ja hyödyllinen teknologia, se ei ole vaihtoehto, johon voimme turvautua joka paikassa. Esimerkiksi

sosiaaliseen mediaan tai työpaikan sähköpostiin kirjauduttaessa tunnistautumiseen ei ole mahdollista käyttää sormenjälkeä, kasvoja tai silmäkuvaa. Tämän takia biometrisen varmennuksen säännölliseen käyttöön on toistaiseksi mahdotonta siirtyä. Mikäli biometristä varmennusta voitaisiin turvallisesti käyttää jokaisessa palvelussa salasanan sijaan, biometriseen varmennukseen siirtyminen voisi jopa toimia.

# 4 SALASANOJEN HALLINTASOVELLUSTYYPPIEN ESITTELY

## 4.1 Yleistä

Salasanojen hallintasovellus on nimensä mukaisesti sovellus, jolla hallitaan salasanoja. Sen päällimmäisenä tarkoituksena on korvata useamman monimutkaisen ja pitkän salasanan muistaminen. Myös tietoturva ja helppokäyttöisyys ovat suuressa roolissa. Salasanojen hallintasovelluksilla on mahdollista generoida, tallentaa sekä hakea salasanoja suojatusta tietokannasta. Suurin osa salasanojen hallintasovelluksista toimii samalla tavalla: Käyttäjää pyydetään luomaan vahva pääsalasana (master password), joka suojaa kaikkia muita salasanoja. (Zamora 2017.) Pääsalasanan luonnin jälkeen käyttäjä voi lisätä hallintasovellukseen kaikki olemassa olevat käyttäjätilinsä. Uusiin palveluihin rekisteröityessään käyttäjä voi käyttää omia salasanojaan tai hallintasovelluksen sisään rakennettua salasanageneraattoria, joka luo satunnaisia, pitkiä sekä turvallisia salasanoja. (Owaida 2020.) Salasanoja voi myös generoida, vaikka ei olisi rekisteroitymässä mihinkään. Esimerkiksi pilvipohjaisen LastPass-hallintasovelluksen verkkosivuilta löytyy salasanageneraattori (kuva 4), jossa käyttäjä voi valita generoitavalle salasanalle erilaisia kriteerejä, kuten salasanan pituus, erilaisten merkkien ottaminen mukaan tai merkkien jättäminen pois.




Kuva 4. LastPass-sivuston salasanageneraattori

## 4.2 Erityyppiset hallintasovellukset

Vaikka salasanojen hallintasovellukset toimivat yleisesti ottaen samalla tavalla, niille on erilaisia käyttötarkoituksia. Yleisimpiä salasanojen hallintasovellusten tyyppejä ovat pilvipohjaiset hallintasovellukset, paikalliset hallintasovellukset sekä selainpohjaiset hallintasovellukset. Seuraavaksi tutkin edellä mainittujen hallintasovellustyyppien ominaisuuksia, hyötyjä sekä haittoja.

### 4.2.1 Pilvipohjaiset hallintasovellukset

Pilvipohjaisessa hallintasovelluksessa käyttäjän kirjautumistietoja pidetään tallessa palveluntarjoajan palvelimella, ja data siirtyy käyttäjän selaimen kautta netin välityksellä korkeasti suojatun viestintäkanavan läpi (Zoho n.d.). Pilvipohjaisten hallintasovellusten suurin hyöty on kirjautumistietojen synkronointi sekä hyvä suojaus. Tämä tarkoittaa sitä, että käyttäjä pääsee käsiksi kirjautumistietoihinsa miltä laitteelta tahansa, ja kirjautumistiedot päivittyvät kaikille laitteille. Jos käyttäjä esimerkiksi lisää hallintasovellukseen uusia tunnuksia tietokoneella, lisätyt tunnukset näkyvät myös puhelimella. Pilvipohjaisesta hallintasovelluksesta esimerkkinä on LastPass.

### 4.2.2 Paikalliset hallintasovellukset

Paikallinen hallintasovellus tarkoittaa, että käyttäjän kirjautumistiedot ovat salauksen takana tallessa käyttäjän järjestelmän paikallisissa tiedostoissa. Toisin kuin pilvipohjaisissa hallintasovelluksissa, paikallissa hallintasovelluksissa kirjautumistiedot ovat ainoastaan käyttäjän omassa hallussa. Paikallisten hallintasovellusten hyvä puoli on, että käyttäjä on itse vastuussa omasta tietoturvastaan, eli kirjautumistiedot eivät ole esimerkiksi palveluntarjoajan käsissä. Paikallisuus koituu tosin myös huonoksi puoleksi, sillä paikallisia hallintasovelluksia ei voi useimmiten käyttää eri laitteiden välillä. Esimerkiksi puhelimella palveluun kirjauduttaessa käyttäjä ei välttämättä muista salasanaansa, joka on ainoastaan tietokoneella tallessa. Paikallisesta hallintasovelluksesta esimerkkinä on KeePass.

### 4.2.3 Selainpohjaiset hallintasovellukset

Selainpohjainen hallintasovellus on nimensä mukaisesti selaimessa toimiva hallintasovellus. Ideana on, että käyttäjän ei tarvitse ladata kolmannen osapuolen hallintasovellusta, vaan hallintasovellus löytyy jo valmiiksi käyttäjälle tutusta selaimesta. Esimerkiksi Mozilla Firefox -selaimesta löytyy selaimen sisään rakennettu Firefox Lockwise -hallintasovellus. Selainpohjaiset hallintasovellukset ovat yleensä erittäin helppokäyttöisiä. Selainpohjaisista hallintasovelluksista löytyy myös laitteiden välinen synkronointi sekä pilvipohjainen tallennus. Ongelmana on, että selainpohjaiset hallintasovellukset eivät ole yhtä joustavia kuin kolmannen osapuolen hallintasovellukset, jotka toimivat selaimesta riippumatta. (Hoffman 2020.) Esimerkiksi tietokoneellaan Firefox-selainta käyttävä käyttäjä ei pääse salasanoihinsa käsiksi puhelimen Google Chrome- tai Safari-selaimen kautta. Selainpohjaisesta hallintasovelluksesta esimerkkinä on Firefox Lockwise, jonka tuki loppui vuonna 2021.

# 5 HALLINTASOVELLUSTEN LÄPIKÄYNTI JA VERTAILU

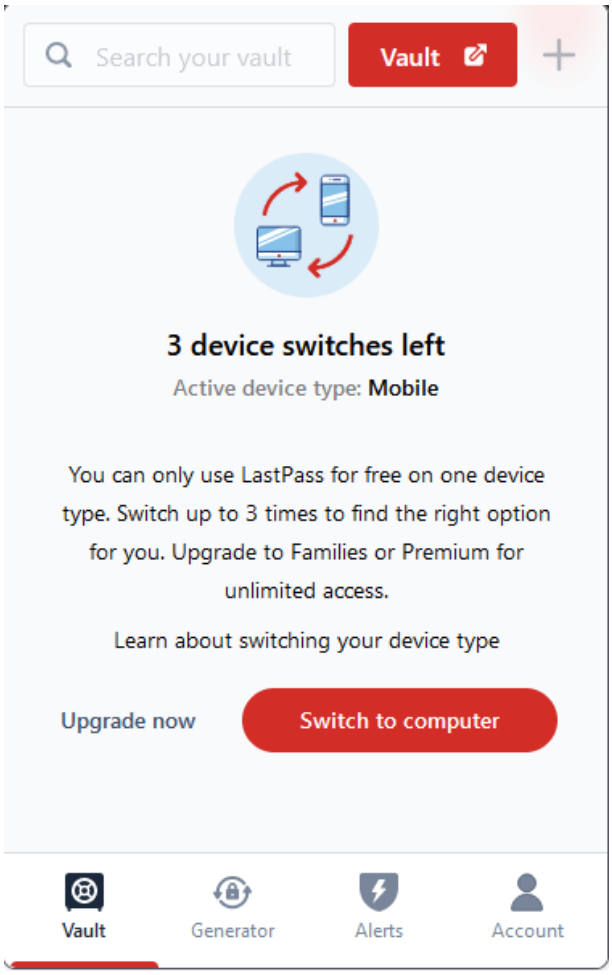
Tässä kappaleessa perehdyn tarkemmin pilvipohjaisten ja paikallisten hallintasovellusten toimintaan ottamalla käyttöön kustakin hallintasovellustyypistä yhden sovelluksen. Tämän jälkeen tutkin hallintasovellusten erilaisia ominaisuuksia ja vertailen niitä keskenään. Selainpohjaisia hallintasovelluksia en käy läpi siksi, että niiden turvallisuus sekä versiotuki ovat nykyään kyseenalaisia.

## 5.1 LastPass

LastPass on neljän tietoturvamielisen ystävän vuonna 2008 perustama pilvipohjainen salasanojen hallintasovellus, jonka tarkoituksena on olla käytettävissä missä vain ja milloin vain (LastPass n.d.). Hallintasovellusta voi käyttää sekä tietokoneella että mobiililaitteilla. Olen itse käyttänyt LastPassia jo jonkin aikaa aktiivisesti, sillä halusin tehdä jotain konkreettista suojatakseni verkkotietoni entistä paremmin. Suojaamisella tarkoitan sitä, että kun salasanoja ei tarvitse itse edes muistaa, niin jokaiseen verkkopalveluun voi ottaa käyttöön vahvan ja monimutkaisen salasanan, joka on käytännössä mahdoton arvata tai murtaa brute force -hyökkäyksellä. Eniten olen henkilökohtaisesti pitänyt LastPassin selkeästä käyttöliittymästä ja helppokäyttöisyydestä. Väripaletti on myös yksinkertainen ja silmää miellyttävä; mustaa, valkoista sekä punaista.

Mielestäni LastPassin ainoa huono puoli on, että ilmaisversiossa on ollut vuodesta 2021 asti mahdollista käyttää sovellusta vain yhdellä laitetyypillä kerrallaan (LastPass n.d.). Käyttäjä pääsee siis käsiksi salasanoihinsa ainoastaan esimerkiksi mobiililaitteella kuten puhelimella tai tabletilla, kun taas tietokone ilmoittaa aktiivisen laitetyypin olevan mobiili (kuva 5). Tämä tarkoittaa sitä, että jos käyttäjä on työmatkalla toisella puolella maailmaa työkoneensa kanssa, ja hänen päälaitteensa on kotona oleva henkilökohtainen tabletti, hän ei silloin pääse ilmaisversiolla työkoneellaan käsiksi salasanoihinsa. Hyvänä puolena on, että ilmaisversiossa tarjotaan kuitenkin kolme kappaletta aktiivisen laitteen vaihtoja, eli edellä mainitussa esimerkissä käyttäjä ei ole heti pulassa, mikäli hänellä on vielä laitevaihtoja jäljellä. LastPassin premium-versio

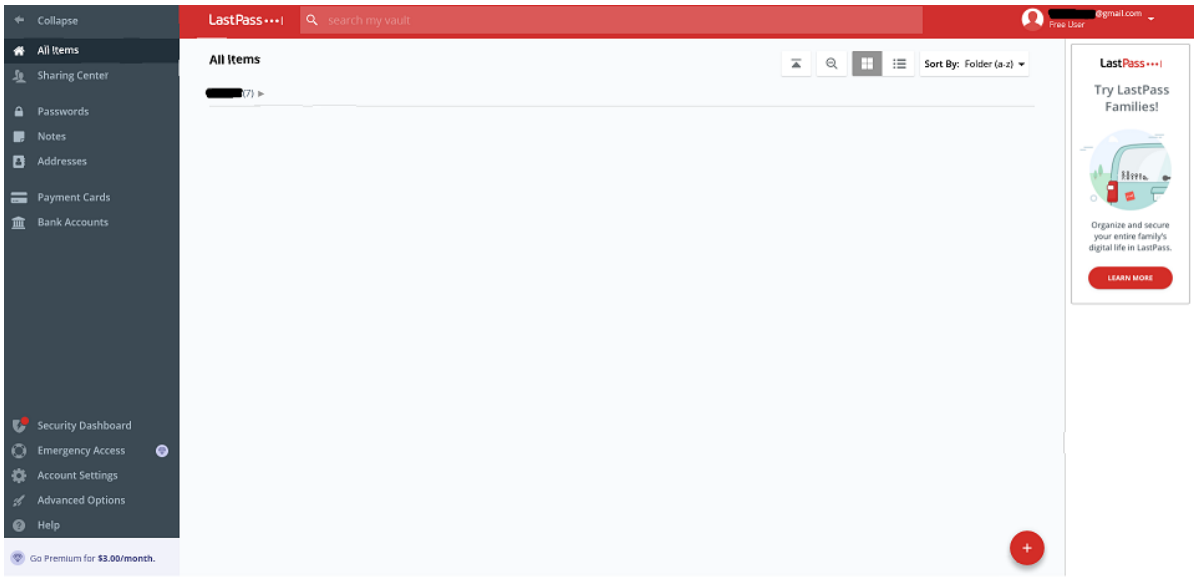
maksaa vain kolme euroa kuukaudessa, joka on mielestäni pieni hinta tietoturvasta ja muista verkkoelämää helpottavista ominaisuuksista.




Kuva 5. LastPassin ilmaisversion ilmoitus aktiivisesta laitetyypistä sekä jäljellä olevien laitevaihtojen määrästä

### 5.1.1 Käyttöliittymä

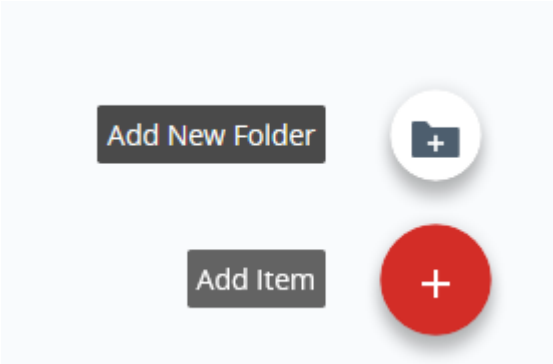
LastPassin ilmaisversiossa sovellusta on mahdollista käyttää ainoastaan selaimen lisäosana, kun taas maksullisesta versiosta löytyy myös mahdollisuus työpöytäsovellukseen. Näillä ei käytännössä ole muuta eroa, kuin käyttäjätunnusten ja salasanojen automaattinen täyttö selaimen ulkopuolella. LastPassin käyttöliittymä itsessään on mielestäni hyvin silmää miellyttävä ja helposti ymmärrettävä, ja oletusnäkymästä löytyy jo pikaisesti kurkkaamalla kaikki peruskäyttöön tarvittavat asiat (kuva 6).




Kuva 6. LastPassin käyttöliittymän oletusnäkymä

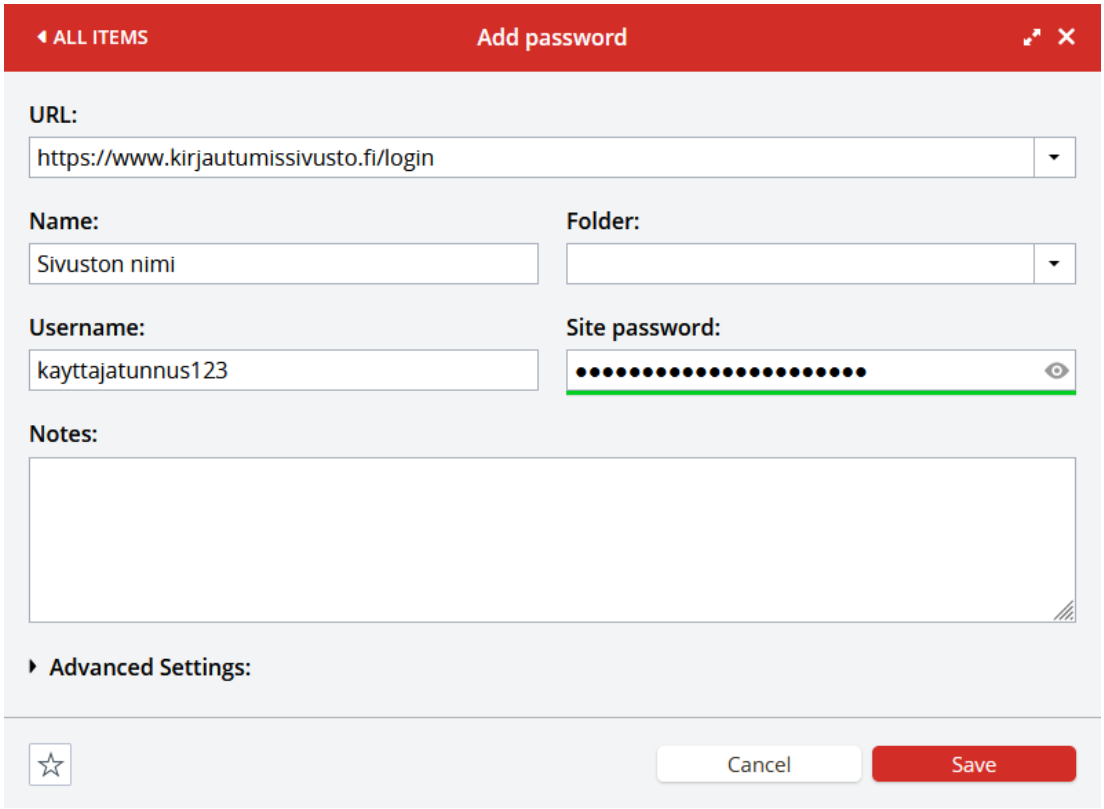
### 5.1.2 Ominaisuudet

Sovellukseen on mahdollista lisätä käyttäjätunnusten ja salasanojen lisäksi myös muun muassa muistilappuja, osoitteita, maksukortteja, sekä pankkitilejä. Tässä esimerkissä lisään satunnaiselle sivustolle uuden käyttäjätunnuksen ja salasanan. Aloitan siirtymällä käyttöliittymän vasemmassa reunassa olevaan Passwords-kohtaan. Oikeasta alareunasta löytyy punainen +-nappula, ja kun sen päälle vie hiiren, käyttäjä voi valita, haluaako hän luoda uuden kansion vai tiedon (kuva 7). Sama valinta löytyy aina riippumatta siitä, mitä tietoa käyttäjä on lisäämässä. Tässä kohtaa klikkaan punaista nappulaa, eli “Add Item”.



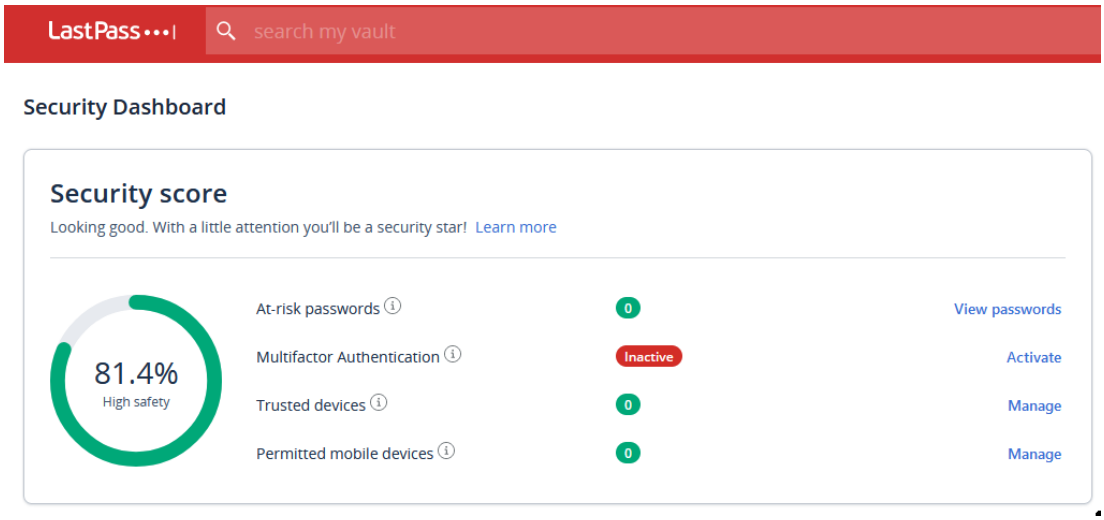

Kuva 7. Uuden tiedon lisääminen LastPassiin

Tämän jälkeen aukeaa näkymä, johon syötetään sivuston verkko-osoite, nimi, käyttäjätunnus ja salasana (kuva 8). Salasanakohta (“Site password”) näyttää salasanan vahvuuden värien avulla, jotka ovat punainen, keltainen ja vihreä. Punainen on melko heikko, kun taas vihreä on vahva, ja keltainen luonnollisesti jotain siltä väliltä. Tässä kohtaa käyttäjän on mahdollista päättää, mihin kansioon salasana tallennetaan, tai käyttäjä voi myös luoda Folder-kohdasta täysin uuden kansion. Tämä on erityisen hyödyllistä esimerkiksi työasioiden ja vapaa-ajan erottelussa, jolloin käyttäjällä on työtunnukset ja vapaa-ajan tunnukset erillisissä kansioissa.



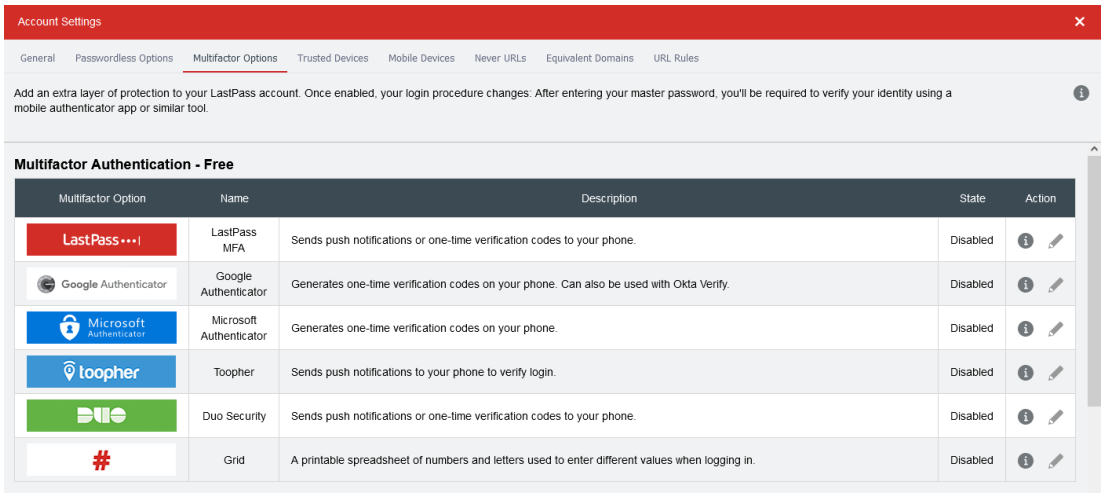

Kuva 8. Uuden käyttäjätunnuksen ja salasanan lisääminen LastPassiin

LastPassin vasemmasta alareunasta löytyy myös kohta “Security Dashboard”, joka tarjoaa tietoturva-arvion, joka kertoo käyttäjälle hänen turvallisuuspisteensä prosenteissa nollasta sataan (kuva 9). Arvio koostuu muun muassa heikoista tai uudelleenkäytetyistä salasanoista sekä monivaiheisen tunnistautumistavan käytöstä.




Kuva 9. LastPassin Security Dashboard

Samaisesta vasemmasta alareunasta, hieman Security Dashboard -kohdan alta, löytyy kohta "Account Settings". Täältä löytyy valikko "Multifactor Options", josta on mahdollista ottaa käyttöön paremman tietoturvan vuoksi monivaiheinen tunnistautuminen (kuva 10). Tunnistautumistapoja ovat esimerkiksi LastPassin oma monivaiheinen tunnistautuminen sekä suosittu Google Authenticator. Sovelluksesta löytyy myös oma salasanageneraattori, jolla on mahdollista määrittää generoitavaan salasanaan tiettyjä kriteereitä, kuten salasanan pituus, kirjainkoko sekä erikoismerkkien käyttö. Tämä ominaisuus löytyy myös LastPassin verkkosivuilta.




Kuva 10. Ilmaisversion mahdolliset monivaiheisen tunnistautumisen tavat

### 5.1.3 Yhteenveto

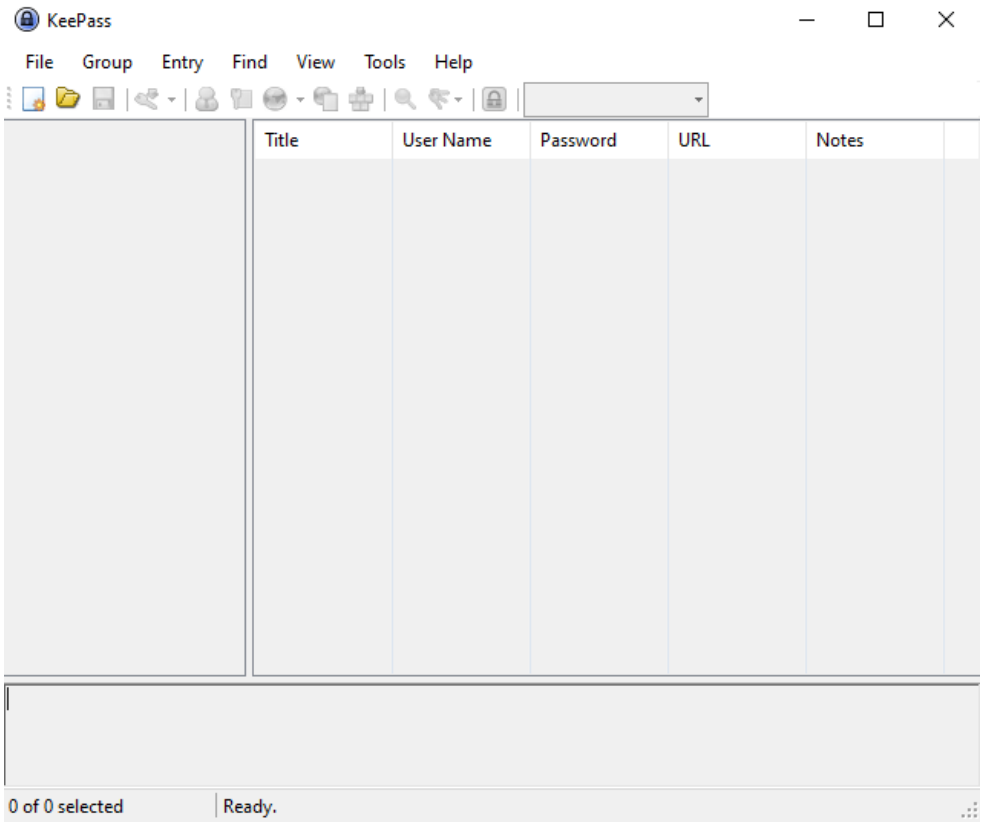
LastPass on mielestäni hyvä valinta sekä aloittelijalle että kokeneemmalle tietokoneen käyttäjälle. Yksinkertainen ja selkeä käyttöliittymä luo helppokäyttöisen, mutta myös hyvin monipuolisen ja kustomoitavan käyttäjäkokemuksen. Monivaiheinen tunnistautuminen tarjoaa ylimääräisen kerroksen tietoturvaa, jolloin käyttäjän arkaluonteiset tiedot pysyvät hyvin turvassa. Suosittelen LastPassin käyttöä pääasiassa maksullisen version kantilta, mikäli tätä hallintasovellusta on tarkoitus käyttää useammalla eri laitetyypillä. Ilmaisversiossa käy helposti niin, että käyttäjän laitetyypiksi on määritetty tietokone, ja yhtäkkiä hänen tarvitseekin kirjautua puhelimellaan johonkin palveluun, ja kirjautumistietoihin pääseekin käsiksi ainoastaan tietokoneella. Mikäli LastPassia on tarkoitus kuitenkin käyttää ainoastaan yhdellä laitetyypillä, ilmaisversio on käytännössä moitteeton.

## 5.2 KeePass

KeePass on ilmainen, avoimen lähdekoodin paikallinen hallintasovellus, jonka on kehittänyt Dominik Reichl. Se on virallisesti saatavilla ainoastaan tietokoneelle, mutta niin sanottuja epävirallisia portteja löytyy myös mobiililaitteille. Kuten paikallisen hallintasovelluksen termistä voi päätellä, sovellus on verkon sijaan paikallisesti käyttäjän tietokoneella, ja näin ollen sovellusta voi käyttää myös ilman verkkoyhteyttä. KeePass on itselleni töistä tuttu sovellus, ja kuten LastPass, se on myös erittäin helppokäyttöinen, joskin käyttöliittymä on hieman vanhahtava.

### 5.2.1 Käyttöliittymä

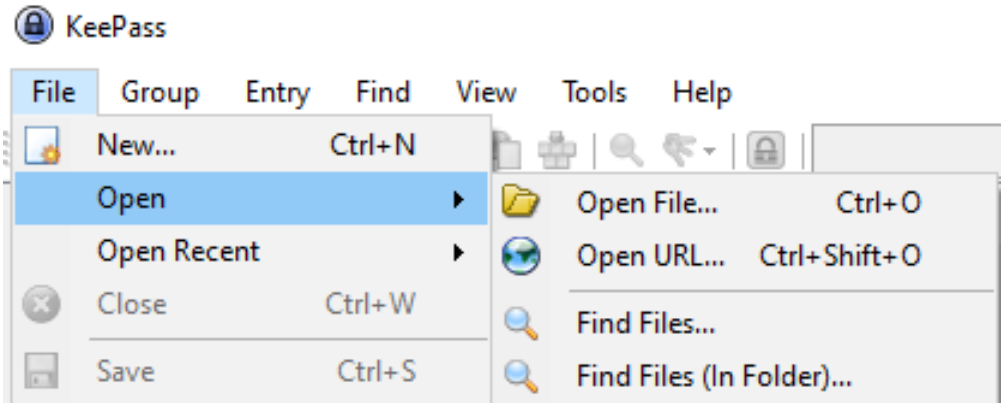
KeePassin käyttöliittymä on mukavan yksinkertainen (kuva 11); kaikki valinnat löytyvät yläreunan pudotusvalikoiden sisältä. Pudotusvalikoiden alapuolelta löytyy yleisiä pikakuvakkeita, kuten uuden tietokannan luonti tai jo olemassa olevan tietokannan avaus. Käyttöliittymä ei ole kovin moderni, mutta pidän siitä itse, ja samaan aikaan se mahdollistaa helpon käyttökokemuksen.




Kuva 11. KeePassin käyttöliittymä

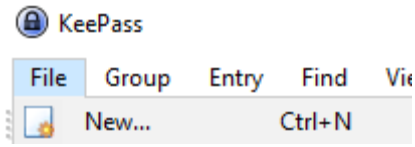
### 5.2.2 Ominaisuudet

KeePass on tarkoituksella minimalistinen, joten ominaisuuksia ei löydy montaa. Tärkein ominaisuus on luonnollisesti tietokantojen eli käyttäjätunnusten ja salasanojen hallinta. Pienempiä, käyttökokemusta helpottavia ominaisuuksia ovat muun muassa pikanäppäimet, salasanageneraattori sekä erilaiset haut, kuten useampaan kertaan käytettyjen salasanojen etsintä. Pikanäppäimet mahdollistavat sen, että käyttäjä voi nopeasti näppäimistöllään syöttää esimerkiksi näppäinyhdistelmän CTRL + N, joka luo uuden tietokannan. CTRL + O puolestaan avaa jo olemassa olevan tietokannan. Pikanäppäimiä löytyy ympäri käyttöliittymän valikoita (kuva 12).



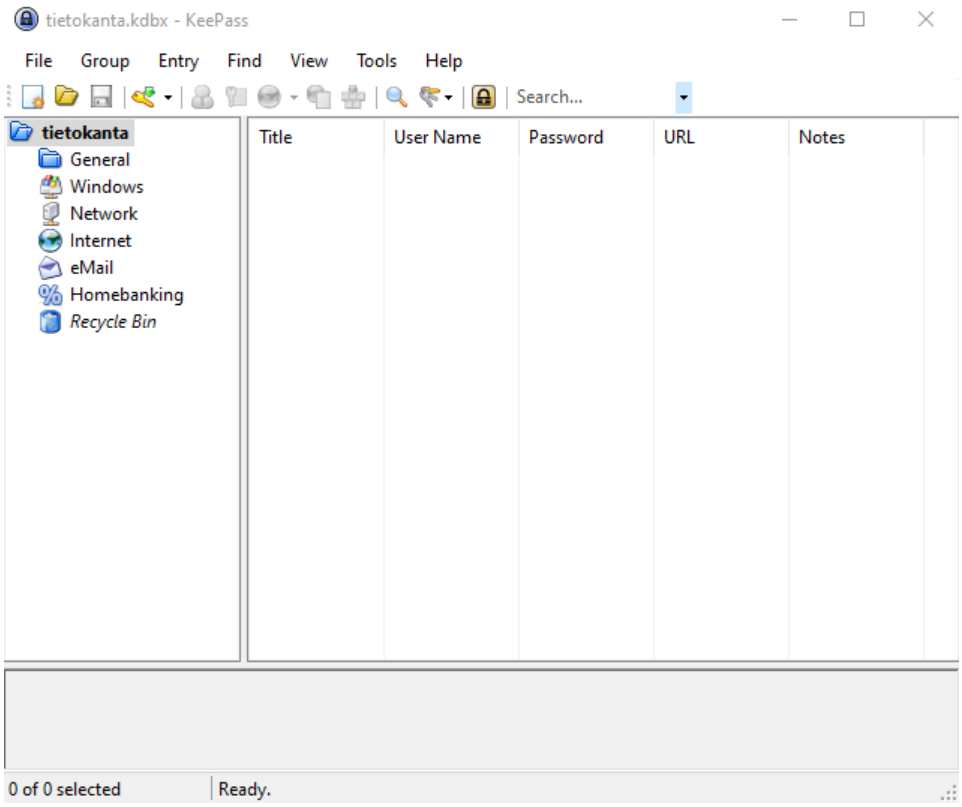

Kuva 12. KeePassin erilaisia toimintoja ja pikanäppäimiä

Tässä esimerkissä luon uuden tietokannan, johon lisään kuvitteelliset tunnukset. Käyttöliittymän vasemmasta yläreunasta löytyy pudotusvalikko “File”, ja sen alta “New” (kuva 13). Seuraavaksi sovellus pyytää käyttäjää määrittämään, minne tietokanta tallennetaan.



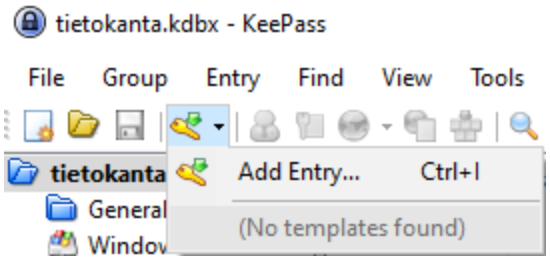

Kuva 13. Uuden tietokannan luonti

Tietokannan tallennuksen jälkeen määritetään pääsalasana, ja tämän jälkeen tietokannan ryhmälle annetaan nimi. Ryhmän nimi voi olla vaikkapa vapaa-aika tai työ, jolloin on selvää, minkälaisia tunnuksia ryhmä sisältää. Yhden tietokannan, eli tietokoneelle tallennetun .kdbx-tiedostopäätteen, alla voi olla useampi ryhmä. Seuraavaksi aukeaa näkymä, jossa juuri luotu tietokanta on auki, ja ryhmän nimenä on “tietokanta” (kuva 14).



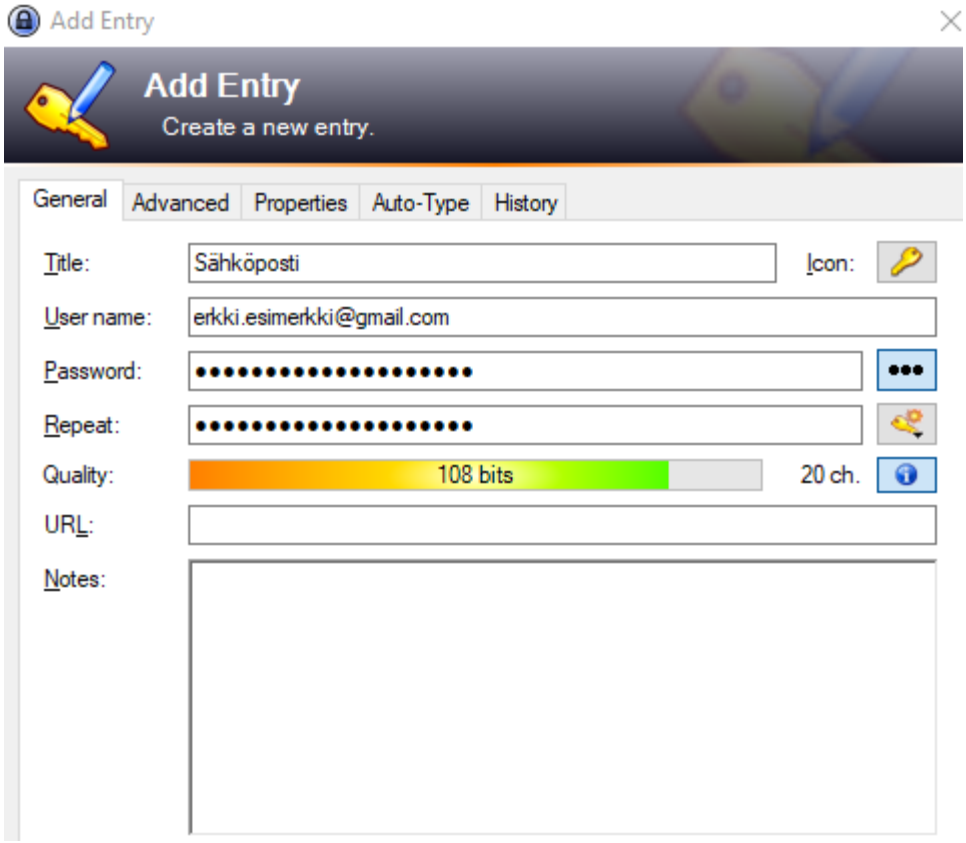

Kuva 14. Näkymä juuri luodusta tietokannasta

Vasemmasta yläreunasta löytyy avainlogon näköinen ominaisuus “Add Entry”, eli uuden tiedon lisääminen tietokantaan (kuva 15).



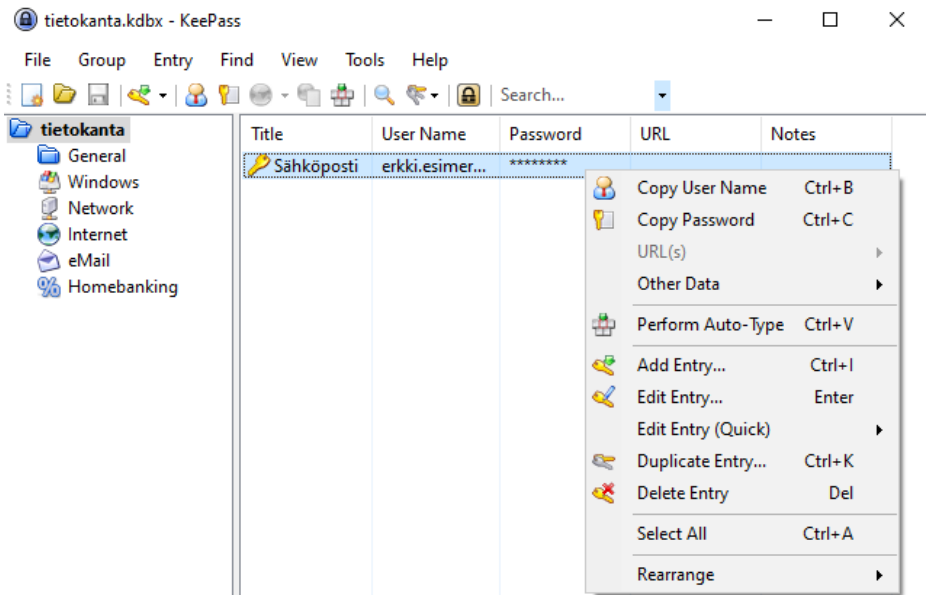

Kuva 15. Uuden tiedon lisääminen tietokantaan

Seuraavaksi aukeaa näkymä, johon käyttäjän tulee syöttää otsikko, käyttäjätunnus sekä salasana (kuva 16).




Kuva 16. Tieto, johon käyttäjä syöttää käyttäjätunnuksen ja salasanan

Tiedon lisäämisen jälkeen se löytyy kätevästi käyttöliittymän keskiosasta (kuva 17). Hiiren oikealla näppäimellä saa näkyviin valikon, jonka kautta voi kopioida käyttäjätunnuksen ja salasanan, tai vaikkapa laittaa sovelluksen syöttämään kyseiset tiedot automaattisesti.




Kuva 17. Juuri lisätty tieto

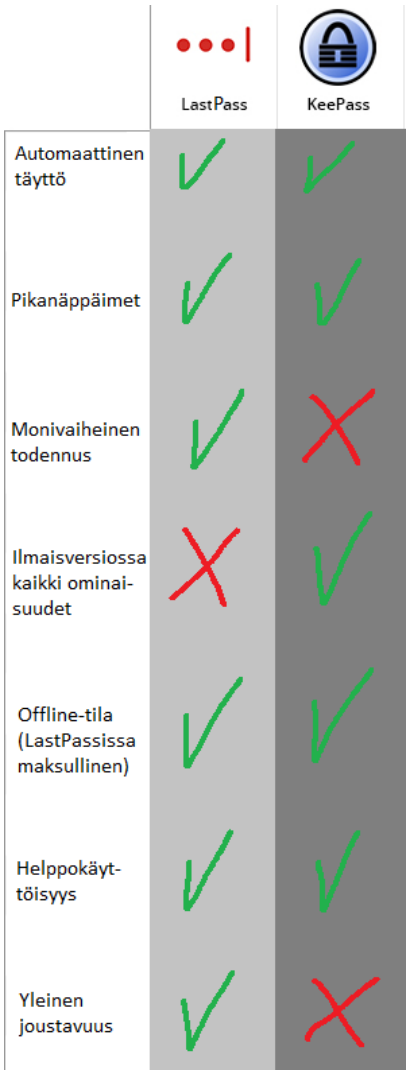
### 5.2.3 Yhteenveto

KeePass on minimalistinen ja kätevä paketti, joka on vieläpä täysin ilmainen. Ominaisuuksia ei ole liikaa, joten jokainen ominaisuus tuntuu merkityksellisemmältä. Suosittelen tätä hallintasovellusta, mikäli käyttäjää ei haittaa, että salasanoihin pääsee käsiksi ainoastaan tietokoneella, ellei käyttäjä halua sählätä epävirallisten porttien kanssa mobiililaitteellaan. Salasanatiedosto on myös mahdollista kopioida muistitikulle, ja näin ollen tiedoston saa auki esimerkiksi mummon tietokoneella, kunhan KeePass on asennettuna. Monivaiheista todennusta KeePassista ei löydy, joten tässä luotetaan lähinnä käyttäjän omiin tietoturvataitoihin.

## 5.3 Paras hallintasovellustyyppi

Vaikka kaikissa hallintasovellustyypeissä on omat riskinsä, kaikki riskit eivät ole yhtä kriittisiä. Pilvipohjainen kolmannen osapuolen hallintasovellus LastPass koki tietomurron vuonna 2015, mutta salattuihin tietoihin, kuten käyttäjien pääsalasanoihin, ei päästy käsiksi (LastPass n.d.). Myös paikalliseen hallintasovellukseen, KeePassiin, liittyy riskejä, kuten monivaiheisen todennuksen puuttuminen sekä tietokoneen hajoaminen, mikäli tietokantaa ei ole kaiken varalta tallennettu muistitikulle tai pilveen.

LastPassin ja KeePassin ominaisuuksien vertailun (kuva 18) perusteella olen itse sitä mieltä, että monipuolisin, joustavin ja turvallisin hallintasovellustyyppi on kolmannen osapuolen pilvipohjainen hallintasovellus. Vaikka pienemmät ominaisuudet, kuten automaattinen täyttö sekä pikanäppäimet löytyvät käytännössä kaikista hallintasovelluksista, mielestäni lisätty tietoturvakerros monivaiheisen todennuksen avulla sekä saumaton toiminta eri laitetyyppien välillä ovat kaikista tärkeimpiä ominaisuuksia.




Kuva 18. LastPassin ja KeePassin ominaisuuksien vertailua

# 6 LOPPUSANAT

Opinnäytetyön aihe oli mielenkiintoinen, ja huomattava osa aiheesta oli itselleni uutta. Oli mukavaa oppia lisää salasanojen tietoturvakäytännöistä sekä salasanojen hallintasovelluksista. Otin LastPassin henkilökohtaiseen käyttöön opinnäytetyön tekemisen aikana ja opin siitä paljon uutta, ja sovelluksen käyttö helpottui sen ansiosta entisestään. Nyt tiedän myös enemmän eri hallintasovellustyyppien hyödyistä ja haitoista. Tämän opinnäytetyön aikana opituista asioista sai hyvät eväät sekä henkilökohtaiseen että työhön liittyvään elämään.

LÄHTEET

Anthony, S. 2014. Facebook's facial recognition software is now as... Viitattu 14.1.2021. https://www.extremetech.com/extreme/178777-facebooks-facial-recognition-software-is-now-as-accurate-as-the-human-brain-but-what-now

Armerding, T. 2019. Password alternatives: Time to do away with passwords? Viitattu 7.1.2021. https://www.synopsys.com/blogs/software-security/password-alternatives/

Castro, C. 2019. HYPR Releases 2.5-year Password Usage Study. Viitattu 7.1.2021. https://www.hypr.com/hypr-password-study-findings/

Cranor, L. 2016. Time to rethink mandatory password changes. Viitattu 11.1.2021. https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes

CyberAvengers 2019. Why Computer Passwords Are Still a Problem in 2019. Viitattu 28.11.2020. https://www.nextgov.com/cybersecurity/2019/01/why-computer-passwords-are-still-problem-2019/154086/

Foster, B. 2020. The History of Passwords, and How We're Making Passwords History. Viitattu 25.11.2020. https://www.mobileiron.com/en/blog/the-history-of-passwords-and-making-passwords-history

Hoffman, C. 2020. Why You Shouldn't Use Your Web Browser's Password Manager. Viitattu 20.1.2021. https://www.howtogeek.com/447345/why-you-shouldnt-use-your-web-browsers-password-manager/

Imperva n.d. What is Two Factor Authentication. Viitattu 9.1.2021. https://www.imperva.com/learn/application-security/2fa-two-factor-authentication/

Lacort, J. 2016. Digital Security: 5 Alternatives to Passwords. Viitattu 4.1.2021. https://www.bbvaopenmind.com/en/technology/digital-world/digital-security-5-alternatives-to-passwords/

Lastpass n.d. 10th Anniversary. Viitattu 24.5.2023. https://www.lastpass.com/10th-anniversary

Lastpass n.d. Changes to LastPass Free. Viitattu 24.5.2023. https://support.lastpass.com/s/document-item?language=en_US&bundleId=lastpass&topicId=LastPass/changes-lastpass-free-plan.html&_LANG=enus

Lastpass n.d. What Happens if LastPass Gets Hacked. Viitattu 21.1.2021. https://www.lastpass.com/security/what-if-lastpass-gets-hacked

Mitchell, A. 2015. The Dynamics of Passwords. Viitattu 2.1.2021. https://blog.sucuri.net/2015/02/the-history-of-passwords.html

Owaida, A. 2020. What is a password manager and why is it useful? Viitattu 16.1.2021. https://www.welivesecurity.com/2020/06/26/what-is-password-manager-why-is-it-useful/

Rawlson, K. 2013. Explainer: Retinal Scan Technology. Viitattu 13.1.2021. https://www.biometricupdate.com/201307/explainer-retinal-scan-technology

Rouse, M. 2017a. What is password? Viitattu 27.11.2020. https://searchsecurity.techtarget.com/definition/password

Rouse, M. 2017b. What is biometric authentication? Viitattu 30.11.2020. https://searchsecurity.techtarget.com/definition/biometric-authentication

Symanovich, S. 2019. How does facial recognition work? Viitattu 13.1.2021. https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html

Zamora, W. 2017. Why you don’t need 27 different passwords. Viitattu 16.1.2021. https://blog.malwarebytes.com/101/2017/05/dont-need-27-different-passwords/

Zoho n.d. Different types of password managers. Viitattu 19.1.2021. https://www.zoho.com/vault/educational-content/different-types-of-password-managers.html