VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Mika Yli-Panula

SALASANAHALLINTAOHJELMIEN VERTAILU

Liiketalous
2022

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

TIIVISTELMÄ

Tekijä	Mika Yli-Panula
Opinnäytetyön nimi	Salasanahallintaohjelmien vertailu
Vuosi	2022
Kieli	suomi
Sivumäärä	38
Ohjaaja	Antti Mäkitalo

Nykyään ihmisillä voi olla lukuisia salasanoja, joita tarvitaan eri palveluihin. Tavanomaisin keino käyttäjän tunnistamiseen verkkopalveluihin kirjautuessa on käyttäjätunnus-salasanayhdistelmä. Salasanojen hallinnoimisen ja muistamisen tueksi on kehitetty salasanahallintaohjelmia, koska suurien salasanamäärien muistaminen on haastavaa. Tässä opinnäytetyössä tutkittiin ja vertailtiin kolmea eri salasanahallintaohjelmaa. Vertailuun valitut ohjelmat ovat KeePassXC, Bitwarden ja Google Password Manager.

Tämän työn teoriaosuus koostettiin verkosta kerätystä materiaalista. Teoriaosuudessa pohjustetaan tekniikoita ja käsitteitä, jotka liittyvät salasanahallintaohjelmiin, kuten tunnistaminen, tietojen salaus, salasanat itsessään sekä niiden varastaminen, murtaminen ja säilöntä. Vertailtavaksi on otettu ohjelmia, joissa salasanojen säilöntämenetelmä ja ohjelmien käyttötapa eroavat toisistaan. Vertailu on toteutettu tutkimalla ohjelmia käyttövaiheittain asennuksesta itse ohjelman käyttöön asti. Ohjelmista on laadittu ominaisuustaulukko, jota on hyödynnetty ohjelmia vertailtaessa.

Vertailun tuloksena saatiin selville, että salasanahallintaohjelmat tekevät salasanojen hallinnoimisesta helpompaa ja parantavat käyttäjän tietoturvaa merkittävästi. Yksiselitteisesti on vaikea todeta mikä vertailtavista ohjelmista on paras, koska siihen vaikuttavat käyttäjän tarpeet ja vaatimukset. Aiheesta voisi tehdä jatkotutkimusta esimerkiksi ottamalla vertailuun mukaan maksullisia salasanahallintaohjelmia.

Avainsanat salasanat, salasanahallintaohjelmat, tunnistaminen, salaus

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietojenkäsittely

ABSTRACT

Author	Mika Yli-Panula
Title	Comparing Password Managers
Year	2022
Language	Finnish
Pages	38
Name of Supervisor	Antti Mäkitalo

Today, people can have numerous passwords that are needed for different services. The most common way to identify a user when logging in to online services is through a username-password combination. Password managers have been developed to support password management and remembering passwords because it is challenging to remember a large number of passwords. In this thesis, three different password managers were studied and compared. The programs selected for the comparison are KeePassXC, Bitwarden, and Google Password Manager.

The theoretical section of this work was compiled from material collected online. The theory section introduces technologies and concepts related to password managers such as authentication, encryption, passwords themselves, and their theft, cracking, and storage. Programs with different methods of storing passwords and how they are used have been compared. The comparison has been carried out by studying the programs step-by-step, from installation to use. A feature table was compiled, which was used in the comparison of the programs.

As a result of the comparison, it was discovered that password managers make password management easier and significantly improve user information security. Unequivocally, it is difficult to establish which of the compared programs is the best since it is affected by the needs and requirements of the user. Further research on the topic could be carried out, for example, by including paid password managers in the comparison.

Keywords passwords, password managers, authentication, encryption

SISÄLLYS

KUVA- JA TAULUKKOLUETTELO

1 JOHDANTO

Suurien salasanamäärien muistaminen on haastavaa. Nykyään ihmiset käyttävät verkossa monia eri palveluita, joiden käyttö edellyttää tilin luomista. Tavanomaisin keino käyttäjän tunnistamiseen verkkopalveluihin kirjautuessa on käyttäjätunnus-salasanayhdistelmä. Uutta tiliä verkkopalveluun luodessa täytyy keksiä salasana. Kaikkien salasanojen muistamisen helpottamiseksi monet käyttävät samaa salasanaa eri verkkopalveluissa (Google 2019). Tapa on tietoturvan kannalta riskialtista. Salasanojen hallinnoimisen ja muistamisen tueksi on kehitetty salasanahallintaohjelmia.

Opinnäytetyön tarkoituksena on tutkia ja vertailla kolmea eri salasanahallintaohjelmaa. Vertailuun valitut ohjelmat ovat KeePassXC, Bitwarden ja Google Password Manager. Tässä opinnäytetyössä tarkastellaan lähemmin salasanahallintaohjelmia: mitä ne ovat, millaisia ohjelmia on olemassa ja miten ne toimivat. Idea aiheeseen syntyi tarpeesta järjestellä omat salasanat. Toinen syy aiheen valintaan on se, että se koskettaa lähes kaikkia ihmisiä maailmassa. Hyvin monella ihmisellä tulee eteen tilanne, jolloin täytyy keksiä uusi salasana. Aiempaa kokemusta salasanahallintaohjelmista ennen opinnäytetyön aloitusta on vain yhdestä ohjelmasta.

Opinnäytetyön tavoitteina on vertailun perusteella arvioida mikä vertailtavista salasanahallintaohjelmista on paras sekä millä tavalla salasanahallintaohjelmat auttavat tutkimusongelmaan eli tunteeseen, jossa lukuisten salasanojen muistaminen on uuvuttavaa ja stressaavaa.

Opinnäytetyö aloitetaan teoriaosuudella, jossa pohjustetaan tekniikoita ja käsitteitä, jotka liittyvät salasanahallintaohjelmiin. Luvussa 3 kerrotaan tarkemmin salasanahallintaohjelmista, jonka jälkeen luvussa 4 esitellään vertailtavat ohjelmat. Luvussa 5 tehdään vertailu ohjelmien kesken. Viimeisessä luvussa käydään läpi vertailun tulokset salasanahallintaohjelmista sekä pohditaan projektia kokonaisuudessa.

2 TEORIATAUSTA

Tässä osuudessa kerrotaan taustaa tunnistuksesta, tietojen salauksesta, salasanoista itsessään sekä niiden heikkouksista, varastamisesta, murtamisesta ja säilönnästä.

2.1 Sähköinen tunnistus ja tunnistusmenetelmät

Turvallinen asiointi ja palveluiden käyttö verkossa on mahdollista sähköisen tunnistamisen avulla. Sähköisessä tunnistamisessa käyttäjä tunnistetaan etänä verkossa. Tarkoituksena on varmentaa käyttäjän oikea henkilöllisyys ja estää asiointi väärin perustein. (STEK)

Tunnistusmenetelmät eli tavat joilla käyttäjä voidaan tunnistaa, voidaan jakaa karkeasti kolmeen eri kategoriaan:

1. Jotain mitä tiedät eli tietoon perustuva todentamistekijä. Esimerkkejä tälläisistä ovat salasana tai PIN-koodi.
2. Jotain mitä sinulla on hallussa eli hallussapitoon perustuva todentamistekijä. Esimerkkejä tälläisistä ovat tunnuslukulaite, mobiilisovellus tai tunnuslukulista.
3. Jotain mitä olet eli johonkin fyysiseen ominaisuuteen perustuva biometrinen todentamistekijä. Esimerkkejä tälläisistä ovat sormenjälki tai iiris. (Kyberturvallisuuskeskus 2021b)

2.1.1 Vahva sähköinen tunnistautuminen

Vahvassa sähköisessä tunnistautumisessa luotettava toimija takaa käyttäjän henkilöllisyyden tämän tunnistautuessa. Suurin osa vahvasta sähköisestä tunnistautumisesta tapahtuu verkkopankkitunnuksilla ja teleyritysten mobiilivarmenteilla. Myös harvemmin käytetty Digi- ja väestötietoviraston kansalaisvarmenne soveltuu vahvaan sähköiseen tunnistautumiseen. Liikenne- ja viestintävirasto Traficom valvoo tunnistamispalveluja lailla, jonka tavoitteena on

luoda yhteiset pelisäännöt. Lain lähtökohtana on, että palveluiden käyttäjät voivat luottaa tietoturvaan ja yksityisyyden suojaan. Vahva sähköinen tunnistautuminen on käytössä etenkin pankki- ja terveyspalveluissa, joissa vaaditaan asiakkaan henkilöllisyyden varmentamista. Myös muilla aloilla vahvan tunnistamisen käyttö on viimeisten vuosien aikana lisääntynyt, sillä se tekee sähköisestä asioinnista merkittävästi turvallisempaa. Aiemmin usein käytettyä henkilötunnus ja salasana-yhdistelmään perustuvaa käyttäjän tunnistautumista ollaan korvaamassa vahvalla sähköisellä tunnistautumisella. (Signicat 2021)

2.1.2 Kaksivaiheinen tunnistus

Kaksivaiheinen tunnistus on käyttäjätunnuksen ja salasanan lisäksi erillinen tunnistautumiseen käytettävä menetelmä. Tällaisia menetelmiä voi olla esimerkiksi tunnuslukutaulukko tai kertakäyttöinen koodi. Sisäänkirjautumista varten palvelun käyttäjä saa kertakäyttöisen koodin erilliseen laitteeseen tai sovellukseen. Tyypillisesti koodi lähetetään tekstiviestitse puhelimeen. Kaksivaiheinen tunnistus tekee tunnistautumisesta huomattavasti turvallisempaa, kun käyttäjätunnuksen ja salasanan lisäksi tarvitaan toinenkin menetelmä palveluun sisäänkirjautumiseen. Kaksivaiheisen tunnistautumisen heikkoutena se hidastaa palveluun sisäänkirjautumista ja käyttäjän on kannettava mukanaan tunnistautumiseen tarvittavaa välinettä. Myös puhelimen tai välineen kadotessa sekä akun loppuessa kaksivaiheinen tunnistus ja sisäänkirjautuminen ei ole mahdollista. (Lehto 2021)

2.2 Salasana

Salasana on merkkijono, jolla varmistetaan käyttäjän henkilöllisyys todennusprosessin aikana. Salasanoja käytetään yleensä yhdessä käyttäjänimen tai sähköpostin kanssa. Ne on suunniteltu olemaan vain käyttäjän tiedossa ja antavat käyttäjälle pääsyn laitteeseen, sovellukseen tai verkkosivustoon. Salasanan pituus voi vaihdella ja ne voivat sisältää kirjaimia, numeroita ja erikoismerkkejä. Salasanaa kutsutaan joskus salalauseeksi, kun siinä käytetään

useampaa kuin yhtä sanaa. Pelkästään numeerisesta salasanasta voidaan käyttää myös termiä pääsykoodi tai PIN-koodi. (Bacon 2021)

Suurin heikkous salasanoihin liittyen on itse palveluiden käyttäjät ja kuinka he määrittelevät salasanansa. Käyttäjien luomat salasanat eivät usein ole tarpeeksi monimutkaisia ja samoja salasanoja käytetään eri palveluissa. Tämä heikentää merkittävästi tietoturvaa, kun yhden salasanan vuotaminen vaikuttaa toisen palvelun tietoturvaan. Palveluiden käyttäjillä on näin ollen suuri vaikutus omien tiliensä tietoturvaan. Teknisiä apuvälineitä ja sosiaalisia menetelmiä hyödyntäen salasanat on mahdollista selvittää ja murtaa. Käyttäjien paljastuneet heikot salasanat voivat edesauttaa murtajaa selvittämään tavan, jolla salasanat säilötään palveluiden järjestelmään, joka taas helpottaa parempien salasanojen murtamista. (Kyberturvallisuuskeskus, 11)

2.3 Salasanojen murtaminen ja varastaminen

Salasanojen varastamiseen ja hyväksikäyttöön on useita eri tapoja. Tyypillisimmät keinot salasanojen varastamiseen ja murtamiseen ovat haittaohjelmat, sosiaaliset ja tekniset huijaukset sekä palveluiden tietomurrot. Palveluiden käyttäjillä itse on suuri mahdollisuus vaikuttaa omaan tietoturvaan ja näin ehkäistä salasanojensa paljastumista. (Kyberturvallisuuskeskus, 8)

2.3.1 Haittaohjelmat

Haittaohjelmia käytetään yhtenä tavanomaisempana keinona varastaa salasana. Haittaohjelmat tutkivat laitteen tiedostoja, selaimia tai ohjelmia ja löytävät sitä kautta tallenettuja salasanoja. Yksi haittaohjelmista on näppäimistönlukija (englanniksi keylogger), joka perustuu siihen, että se lukee, tallentaa ja toimittaa kaikki käyttäjän kirjoitukset hyökkääjälle. Viruksentorjunta, palomuuri, käyttöjärjestelmä, selaimet ja niiden liitännäiset on hyvä päivittää tasaisin väliajoin. Tällä tavoin pystyy parhaiten välttymään haittaohjelmilta. (Kyberturvallisuuskeskus, 8-9)

2.3.2 Sosiaaliset ja tekniset huijaukset

Erilaisilla huijauksilla yritetään myös varastaa salasanoja. Tietoja voidaan kalastella erilaisin menetelmin: sähköpostitse, puhelimitse, tekstiviestitse tai pikaviestimien välityksellä. Sähköpostihuijaus käytettynä jonkin edellä mainitun muun menetelmän kanssa lisää huijauksen uskottavuutta. Vakuuttavan näköisessä sähköpostihuijausviestissä voidaan esimerkiksi pyytää vaihtamaan salasana sähköpostissa mainitulla linkillä, joka voi näyttää hyvin samankaltaiselta kuin alkuperäinen sivusto. Tietojenkalastelusivustolle kirjoitettu salasana päätyy tälläisissä tapauksissa suoraan huijarille. Työpaikoilla huijari voi esiintyä yrityksen IT-tukihenkilönä, joka kysyy salasanaasi. Todellisuudessa IT-tuen ei ikinä tarvitse tietää salasanaasi. Nyrkkisääntönä on hyvä muistaa, että esimerkiksi pankki tai mikään muukaan taho ei kysy ikinä salasanaasi. (Kyberturvallisuuskeskus, 9)

2.3.3 Tietomurrot

Palveluiden tietomurroissa voi vuotaa isojakin määriä salasanoja riippuen palvelun käyttäjämäärästä. Käytännössä itse käyttäjä pystyy harvoin vaikuttamaan käyttämänsä palvelun tietoturvaan. Palvelukohtaiset ja mahdollisimman pitkät sekä monimutkaiset salasanat yhdessä kaksivaiheisen tunnistuksen kanssa on paras tapa parantaa omaa tietoturvaa. Tällöin tietomurrossa paljastuneista tiedoista on vaikeampi selvittää salasanaa. Palvelukohtaista salasanaa käyttäessä muiden palveluiden käyttöä voi jatkaa normaalisti ja vain murretun palvelun tiedot vaarantuvat. (Kyberturvallisuuskeskus, 9)

2.3.4 Väsytyshyökkäys

Väsytyshyökkäyksessä (englanniksi brute-force attack) käytetään yrityksen ja erehdyksen kautta kaikkia mahdollisia käyttäjätunnus-salasanayhdistelmiä. Tämä on vanha tapa murtaa salasana, mutta hakkereiden keskuudessa se on yhä edelleen suosittu ja tehokas. Yhtenä syynä voidaan pitää sitä, että salasanan

pituudesta ja monimutkaisuudesta riippuen sen murtaminen voi kestää muutamasta sekunnista useisiin vuosiin. (Kaspersky)

2.3.5 Sanakirjahyökkäys

Sanakirjahyökkäystä voidaan käyttää yhtenä väsytyshyökkäystekniikkana, jossa hyökkääjä yrittää arvata sanakirjalistan perusteella salasanaa käyttäen esimerkiksi tiettyjä yleisiä sanoja tai lauseita. Sanakirjahyökkäyksen avulla salasanan varastaminen voi onnistua nopeastikin, jos ihmiset käyttävät yksinkertaisia, helposti muistettavia ja samoja salasanoja useilla eri tileillä. Monet sanakirjahyökkäyksissä käytettävät työkalut hyödyntävät tietomurroista vuotaneita salasanoja sekä sanoja ja lauseita, joissa esimerkiksi kirjain a on korvattu merkillä @ tai numeroita on lisätty salasanan loppuun. Verizonin vuonna 2019 tekemän tutkimuksen mukaan 80% salasanamurroista liittyy varastettuihin ja uudelleen käytettyihin tunnistetietoihin. Parhaiten sanakirjahyökkäystä vastaan pystyy puolustautumaan käyttämällä palvelukohtaisesti pitkiä ja monimutkaisia salasanoja. (Swinhoe 2020)

2.3.6 Sateenkaarihyökkäys

Sateenkaaritaulukossa (englanniksi rainbow table) on salasanoja ja niistä valmiiksi laskettuja tiivisteitä joiden avulla voidaan selvittää mikä selkokielinen salasana vastaa mitäkin tiivistettä. Sateenkaarihyökkäystä varten hyökkääjällä täytyy olla hallussa tietomurrossa vuotaneet salasanatiivisteet, joita verrataan sateenkaaritaulukossa oleviin tiivisteisiin. Kyberrikolliset ovat omaksuneet sateenkaarihyökkäyksen helpoksi tavaksi murtaa salasanoja, koska hyökkääjän tarvitsee vain katsoa sateenkaaritaulukosta oikea salasanatiiviste. Sanakirja- ja väsytyshyökkäykseen verrattuna sateenkaarihyökkäys vaatii vähemmän laskentatehoa ja kovalevytilaa. Täysin uuden sateenkaaritaulukon tiivisteiden laskemiseen kuluu paljon aikaa, mutta verkossa on olemassa valmiiksi laskettuja taulukoita, jotka nopeuttavat salasanan murtamista. Estääkseen sateenkaarihyökkäykset ensisijainen keino on säilöä salasanat suolattuna palvelun

järjestelmässä. Muita keinoja ovat kaksivaiheisen tunnistuksen käyttö, murrettujen salasanatiivistealgoritmien välttäminen palvelussa tai palvelun suunnittelu niin, että siinä ei käytetä salasanaa ollenkaan. (Welekwe 2022)

2.3.7 Internetliikenteen vakoilu

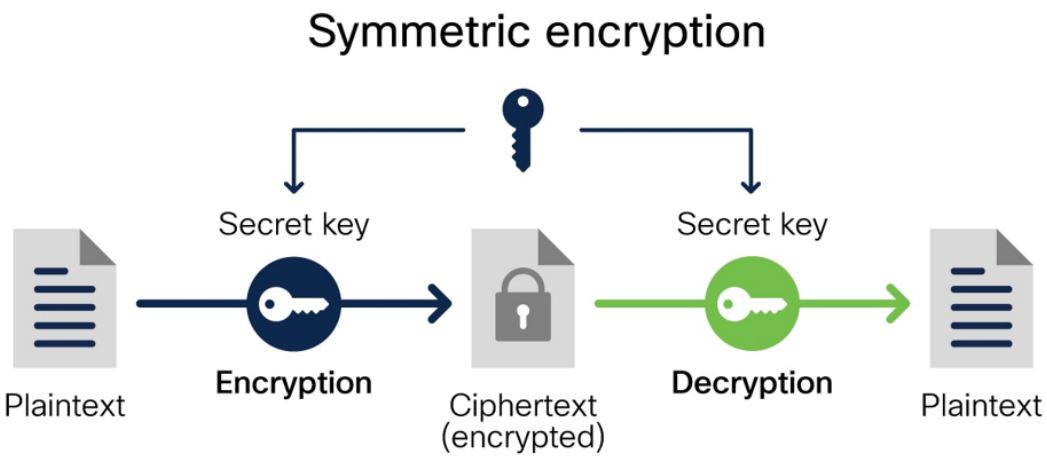
Verkkoliikenne kulkeutuu monen eri palvelimen kautta ennen kuin se yhdistyy valitulle sivustolle. Verkkoliikennettä vakoillessa huijarilla on mahdollista nähdä kaikki, mitä verkossa tapahtuu. Vakoilussa käytetään hyväksi usein julkisia ja suojaamattomia Wi-Fi-verkkoja tai murrettuja internet-reitittimiä. (F-Secure)

VPN-yhteyden avulla voi suojautua internetliikenteen vakoilulta. VPN eli virtual private network on tekniikka, jonka avulla voi suojata verkkoliikenteen salatun yhteyden ansiosta. VPN-yhteys salaa kaiken verkkoliikenteen käyttäjältä VPN-palveluntarjoajalle saakka, piilottaen käyttäjän oikean sijainnin ja IP-osoitteen. (Mikrobitti 2020)

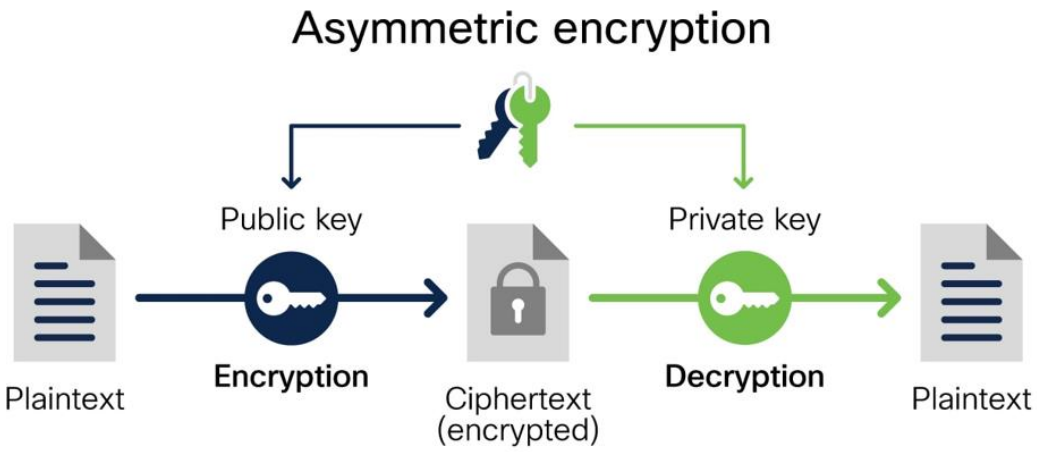
2.4 Salaus

Nykyään arkaluontoisten tietojen siirtäminen tai tallentaminen on osa jokapäivästä elämää. Salaustekniikoiden avulla turvataan sekä siirron aikana liikkuva tieto että tallennettu tieto. Tietojenkäsittelyssä salaus (englanniksi encryption) on menetelmä, jossa tieto muunnetaan selkotekstistä (englanniksi plaintext) koodattuun muotoon salatekstiksi (englanniksi ciphertext). Salauksen purkaminen (englanniksi decryption) on päinvastainen toiminto, jossa salateksti muunnetaan selkotekstiksi. Salauksen purkuun tarkoitetulla avaimella salattua tietoa on mahdollista lukea ja käsitellä. Salaus ei itsessään estä tietojen hakkerointia tai varastamista, vaan se estää varastetun tiedon käytön, koska hakkeri ei näe sitä selkokielisenä. Tietojen salausta on kahta tyyppiä: symmetrinen salaus ja epäsymmetrinen salaus. Symmetrisessä salauksessa on vain yksi salainen avain, joka sekä salaa ja purkaa tiedot (kuva 1). Epäsymmetrisessä salauksessa käytetään kahta avainta, toinen salaukseen ja toinen sen purkuun (kuva 2).

Jaetulla julkisella avaimella salataan tiedot. Jakamattomalla salaisella avaimella saadaan taas purettua tiedot. Symmetrinen salaus on nopeampi kuin epäsymmetrinen salaus, mutta ennen kuin symmetrisen salauksen purkaminen on mahdollista, täytyy vastaanottajan saada salainen avain tiedon lähettäjältä. Tämä johtaa siihen, että organisaatioiden on hallittava turvallisesti valtava määrä avaimia. Epäsymmetrinen salaus on vastaavasti turvallisempi, johtuen kahden eri avaimen käytöstä. (Druva)



Kuva 1. Symmetrinen salaus. (Cisco)



Kuva 2. Epäsymmetrinen salaus. (Cisco)

Symmetristä salausta käytetään esimerkiksi pankkiasioinnissa ja tietojen tallennuksessa. Pankkien arkaluontoisten asiakastietojen salaus on erittäin tärkeää. Salauksen mahdollisimman nopean purkamisen ansiosta symmetrinen salaus soveltuu hyvin pankkien toimintaan sekä tietojen tallennukseen. Epäsymmetristä salausta käytetään esimerkiksi digitaalisissa allekirjoituksissa ja käyttäjän tunnistamisessa kryptovaluuttasiirroissa. Kahden avaimen käytön ansiosta lähetettävän tiedon aitous pystytään vahvistamaan, kun vastaanottava taho tarkistaa tiedon aitouden julkisella avaimella. (Encryption consulting)

2.5 AES-salausalgoritmi

AES tai Advanced Encryption Standard, joka tunnettiin alunperin nimellä Rijndael, on symmetrinen salausalgoritmi, jonka on suunnitelleet belgialaiset kryptografit Joan Daemen ja Vincent Rijmen 90-luvun loppupuolella. Yhdysvaltain kansallinen standardi- ja teknologiainstituutti NIST on valinnut AES-algoritmin alan salausstandardiksi. AES-algoritmiperhe koostuu kolmesta eri algoritmista: AES-128, AES-192 ja AES-256. Algoritmit ovat samankaltaisia, mutta ainoastaan käytetyn avaimen koko muuttuu. Suurin kooltaan eli 256-bittinen on turvallisin kolmesta, mutta vie eniten laskentatehoa. AES on yksi suosituimmista salausalgoritmeista, jota käytetään käytännössä kaikessa tietokoneisiin liittyvässä:

pilvitallennuksessa, VPN:ssä, valtioiden ja yritysten järjestelmissä, joissa vaaditaan varmuus siitä, että tiedot pysyvät yksityisinä ja salassa. (Hougen 2021)

2.6 Salasanojen säilöntä ja salasanatiivisteet

Tietoturvan kannalta on parempi, ettei palvelun tai verkkosivun salasanoja tallenneta järjestelmään selkokielisenä vaan salasanoista lasketaan tiiviste jollakin yksisuuntaisella tiivistefunktiolla. Yksisuuntaisuudella tarkoitetaan sitä, että tiivisteestä ei pystyisi saada selville alkuperäistä salasanaa. Palveluiden huolellisesti laadittu salasanojen säilöntä alentaa riskiä, että salasanat päätyisivät vääriin käsiin. Palveluihin sisäänkirjautuessa järjestelmään tallennettua tiivistettä verrataan kirjoitetun salasanan tuottamaan tiivisteeseen. Järjestelmään tallennetun tiivisteen ja kirjoitetun salasanan tuottaman tiivisteen ollessa samoja palvelu päästää sinut kirjautumaan sisään. Salasanatiivisteiden yksi turvallisuushyöty tulee siinä, että palvelun ei tarvitse tietää käyttäjiensä selkokielisiä salasanoja. Tavallisesti varastaakseen salananan hyökkääjä tarvitsee yleensä haltuunsa salasanatiivisteen, jolloin salasanojen murtaminen ja selvittäminen vaikeutuu olennaisesti, kun murtajan täytyy arvailla oikeaa salasanaa tiivisteiden perusteella. Murtamista helpottaakseen on kehitetty sitä varten toimivia ohjelmia, joilla salasanoja on nopeampaa arvailla tiivisteistä. (Kyberturvallisuuskeskus, 11)

2.7 Salasanatiivistealgoritmit ja kryptografiset tiivistefunktiot

Salasanatiivisteiden muodostamiseen on olemassa lukuisia salasanatiivistealgoritmeja. Salasanatiivistealgoritmit on suunniteltu toimimaan tarkoituksella hitaina, mikä lisää salasanojen turvallisuutta, jolloin salasanojen murtaminen vaikeutuu erityisesti väsytyshyökkäysmenetelmällä. Yleiskäyttöisiin kryptografisiin tiivistefunktioihin verrattuna salasanatiivistealgoritmit ovat merkittävästi hitaampia. Standardoitua kryptografista tiivistefunktiota, kuten esimerkiksi SHA-2:ta hyödynnetään tyypillisesti salasanatiivistealgoritmeissa. Pelkästään yleistä tiivistefunktion käyttöä salasanatiivisteen luomisessa ei

suositella, vaan on hyvä käyttää jotain salasanatiivisteen luomiseen tarkoitettua salasanatiivistealgoritmia. Algoritmeista esimerkiksi PBKDF2, bcrypt tai scrypt ovat hyviä vaihtoehtoja salasanatiivisteen luomiseen. (Kyberturvallisuuskeskus, 11-12)

2.7.1 SHA-2

SHA-2 tulee englanninkielen sanoista Secure Hash Algorithm 2. SHA-2 on joukko kryptografisia tiivistefunktioita, johon kuuluu kuusi eri algoritmia: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 ja SHA-512/256. Numeroilla viitataan bittiarvojen pituuteen. Vuonna 2001 julkaistun SHA-2-algoritmin on suunnittellut Yhdysvaltain tiedusteluelin National Security Agency (NSA). SHA2:ta käytetään muun muassa salausprotokollissa, digitaalisissa varmenteissa ja kryptovaluuttojen siirron vahvistamisessa. SHA-2:ta ei ole vielä tiettävästi murrettu, joten sitä voidaan yleisesti suositella turvalliseen tiivisteen luomiseen. (Lake 2022)

2.7.2 PBKDF2

Salasanatiivistealgoritmi PBKDF2 lyhenne tulee englanninkielen sanoista Password-Based Key Derivation Function 2. Sen on suunnitellut RSA Laboratories. Salasanatiivistealgoritmien kuten PBKDF2:n yhtenä tarkoituksena on tehdä väsytyshyökkäyksen käytöstä vaikeampaa tiivisteiden murtamisessa. Salasanatiivistealgoritmeihin bcryptiin ja scryptiin verrattuna PBKDF2 on helpommin murrettavissa väsystyshyökkäystekniikkaa käyttäessä, koska se vaatii vähemmän muistia algoritmin suorittamiseen. (Gibbs 2016)

2.7.3 Bcrypt

Tietokoneiden laskentatehon kasvaessa väsytyshyökkäystekniikan muodostamien arvauksien määrä on lisääntynyt valtavasti. Salasanatiivistealgoritmi bcrypt on tarkoituksella suunniteltu käyttämään paljon laskentatehoa niin, että nimenomaan väsytyshyökkäystekniikan avulla olisi mahdollisimman vaikea saada selville oikeaa salasanaa tiivisteestä. Bcryptissä voi määritellä tiivisteen muodostamiseen tarvittavan laskentatehon määrää. Näin ollen palveluntarjoaja

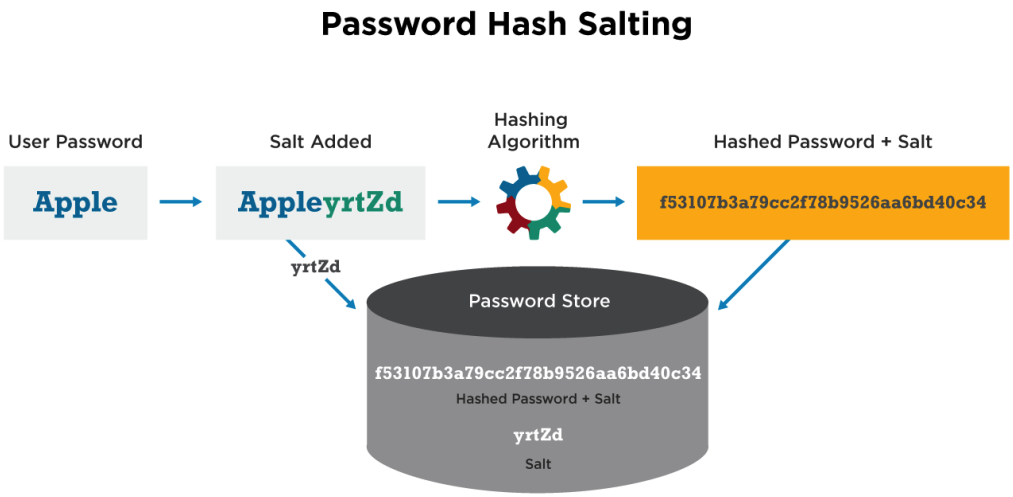
voi asettaa laskentatehon riittävän korkeaksi, jolloin tämän hetken tietokoneiden laskentateholla salasanojen arvailu kestää kuukausista vuosiin tehden siitä aikaa vievää ja kallista. (Gibbs 2016)

2.7.4 Scrypt

Salasanatiivistealgoritmi scrypt on alunperin kehitetty Tarsnap-varmuuskopiointipalvelua varten. Arvion mukaan kun vuoden 2009 laitteistolla käytetään 5 sekuntia tiivisteen laskemiseen, vaaditaan scryptillä muodostaman tiivisteen murtamiseen väsytyshyökkäyksellä 4000-kertainen määrä laskentatehoa bcryptiin verrattuna. PBKDF2-salasanatiivistealgoritmiin verrattuna laskentatehoa tarvitaan jopa 20 000-kertainen määrä. (Tarsnap)

2.8 Salasanan suolaus

Salasanatiivistealgoritmeissä suolan käyttö edistää olennaisesti turvallisuutta. Suola on satunnaisesti generoitu käyttäjäkohtainen yksilöllinen merkkijono, joka lisätään ennen tiivisteen muodostamista käyttäjän antamaan salasanaan (kuva 3). Tällöin tilanteessa, jossa eri käyttäjät antavat identtisen salasanan, on salasanan muodostama salasanatiiviste erilainen suolan ansiosta. Tämä tekee salasanojen murtamisesta huomattavasti hankalampaa tiivisteiden avulla, kun muutaman salasanan selvittäminen ei auta kaikkien salasanojen murtamisessa. Tosin hyökkääjän tietäessä käytetyn suolan ja tiivistefunktion, suolatut salasanatiivisteet ovat murrettavissa. Erikoismerkkien käyttö ja se, mitä tiivistefunktiota käytetään vaikuttavat pidemmän salasanan murtamisessa. (Kyberturvallisuuskeskus, 12)



Kuva 3. Salasanatiivisteen ja suolauksen toimintaperiaate. (Mezquita 2020)

3 SALASANAHALLINTAOHJELMAT

Salasanahallintaohjelmien avulla voi luoda sekä säilöä uniikkeja ja vahvoja salasanoja, jolloin jokaisen eri tilin käyttäjätietoja ei tarvitse muistaa ulkoa. Salasananhallintaohjelmista on olemassa monia ilmaisia sekä maksullisia versioita eri käyttötarpeisiin niin tietokoneille, internetselaimille kuin mobiililaitteille. Kieli- ja alustatuki sekä ominaisuudet vaihtelevat ohjelmittain. Osa ohjelmista tallentaa salasanat paikallisesti tietokoneelle tai sille laitteelle, jolle ohjelma on asennettu. On myös olemassa pilvipalveluissa toimivia salasanahallintaohjelmia, jolloin salasanat ovat synkronoidut ja saatavilla eri päätelaitteiden kesken. (Kyberturvallisuuskeskus 2021a)

Salasanahallintaohjelma tallentaa salasanat salattuun muotoon siten, että pääsy salasanaholviin on yhden pääsalasanan takana. Pääsalasana suojaa näin ollen kaikkia muita salasanoja, joten on erityisen tärkeää asettaa täysin yksilöllinen pääsalasana pienentääkseen mahdollisen tietomurron riskiä. Käyttöönottovaiheessa osa ohjelmista voi antaa palautuskoodin, jolla saa pääsyn takaisin ohjelmaan pääsalasanan unohtuessa. Muutoin ilman tätä ominaisuutta pääsy salasanoihin estyy kokonaan pääsalasanan unohtuessa. Lisäturvaa salasanahallintaohjelmiin tuo kaksivaiheisen tunnistamisen käyttö, mikäli se on mahdollista. Jotkut ohjelmat voivat helpottaa uuden salasanan keksimistä rekisteröintivaiheessa suosittelemalla vahvaa salasanaa. Toinen tyypillinen ominaisuus on salasanojen automaattinen täyttö verkkopalveluihin kirjautuessa. (Kyberturvallisuuskeskus 2021a)

Salasanahallintaohjelman käyttö auttaa suojautumaan monilta vaaroilta, kuten tietomurroilta ja hyökkäyksiltä silloin, kun käytetään tilikohtaisia salasanoja sekä myös salasanojen kalasteluyrityksiltä, sillä osa ohjelmista osaa tunnistaa kirjautumisvaiheessa aidon verkkosivuston osoitteen salasanaa ehdottaessa. Salasanahallintaohjelma ei suojaa sellaisessa tapauksessa, jossa on esimerkiksi annettu pankkitunnukset rikollisten käyttöön. Salasanahallintaohjelmasta voidaan

käyttää myös nimitystä salasanamanageri, salasanaohjelma, salasanojen hallintaohjelma tai salasanojen hallintasovellus. (Kyberturvallisuuskeskus 2021a)

4 OHJELMIEN ESITTELY

Tässä osiossa on esiteltynä kolme salasanahallintaohjelmaa, jotka on otettu vertailtaviksi tähän opinnäytetyöhön. Vertailuun on haluttu mukaan ohjelmia, joiden salasanojen säilöntämenetelmä ja ohjelmien käyttötapa eroavat toisistaan, mikä tekee vertailusta mahdollisimman kattavan.

4.1 KeePassXC

KeePassXC on täysin ilmainen avoimen lähdekoodin salasanahallintaohjelma, jolla voi luoda ja tallentaa salasanoja sekä hallita käyttäjätietoja. KeePassXC toimii Windows-, macOS- ja Linux-alustoilla. KeePassXC on suunniteltu käyttäjille, joilla on erittäin korkeat turvallisuusvaatimukset kirjautumistietojen hallintaa varten. Luotuun tietokantaan voi tallentaa monenlaista tietoa kuten käyttäjänimiä, salasanoja, verkkosivustoja, liitteitä tai muistiinpanoja. Salatun tietokannan voi tallentaa mihin tahansa paikkaan paikallisesti ja varmuuskopiointi on mahdollista omavalintaiseen pilvipalveluun. Tietojen tunnistamisen ja hallinnan helpottamiseksi tallennettuihin tietoihin voi määrittää otsikot ja kuvakkeet. Lisäksi tiedot voidaan lajitella ryhmittäin. Hakutoiminnon avulla löytyvät tarvittavat käyttäjätiedot salasanaholvista nopeasti. Ohjelman salasanageneraattori laatii salasanan millä tahansa merkkiyhdistelmällä tai helposti muistettavalla salalauseella. (KeePassXC)

4.2 Bitwarden

Bitwarden on avoimen lähdekoodin salasanahallintaohjelma, josta on olemassa ilmainen versio karsituilla ominaisuuksilla sekä maksullisia versiota yksityis- tai työkäyttöön (kuva 4 ja 5). Bitwardenin käyttö edellyttää tilin luomista ja sitä voi käyttää useimmilla selaimilla tai niiden laajennuksilla, Windows-, macOS-, Linux-käyttöjärjestelmillä, komentorivikäyttöliittymillä, puhelimilla iOS- tai Android-käyttöjärjestelmillä. Salasanojen lisäksi holviin voi tallentaa myös luottokortti-, henkilöllisyys- tai muistiinpanotietoja. Bitwardenin oman pilvisynkronoinnin

ansiosta tallennettuja tietoja pystyy hallinnoimaan laitteesta tai paikasta riippumatta. Saadakseen täyden kontrollin tietoihin myös oman palvelimen pystyttäminen on mahdollista avoimen lähdekoodin ansiosta. Avoimen lähdekoodin ja bugipalkkio-ohjelman lisäksi turvallisuutta yritetään parantaa teettämällä kolmannen osapuolen tietoturva-auditointeja. (Bitwarden c)

Features for You	Free	Premium	Free Org	Families Org
Bitwarden Core Features	☑	☑	☑	☑
Max Users	1	1	2	6
Sharing through collections	-	-	Max 2 Collections	Unlimited Collections
Bitwarden Send for direct encrypted sharing	Text Only	Text and Files	Text Only	Text and Files
Two-step Login	Email, Authentication App	YubiKey, FIDO2, Duo, Email, Authentication app	Email, Authentication App	YubiKey, FIDO2, Duo, Email, Authentication app
Encrypted File Attachments	-	1GB Personal	-	1GB Personal and 1GB for Organizational Items
Bitwarden Authenticator (TOTP)	-	☑	-	☑
Vault Health Reports	-	☑	-	☑
Emergency Access	-	☑	-	☑
Priority Support	-	☑	-	☑
Self-host Options	☑	☑	-	☑
Pricing	**$0 Get Started**	**$10/Year Get Started**	**$0 Get Started**	**$40/Year Get Started**

Kuva 4. Bitwardenin hinnat yksityiskäytössä. (Bitwarden b)

Compare Business Features and Plans

Features for Business	Teams	Enterprise
Bitwarden Core Features	☑	☑
Premium Features for Users	☑	☑
Unlimited Users	☑	☑
Unlimited Sharing Through Collections	☑	☑
API Access	☑	☑
Directory Connector	☑	☑
Event and Audit Logs	☑	☑
User Groups	☑	☑
Custom Roles	-	☑
Enterprise Policies	-	☑
SSO Integration	-	☑
Free Families Plan for Users	-	☑
Admin Password Reset	-	☑
Self-host Option	-	☑
Included Premium Features		
Bitwarden Send for direct encrypted sharing	Text and Files	Text and Files
Enhanced Two-step Login	YubiKey, FIDO2, Duo	YubiKey, FIDO2, Duo
Encrypted File Attachments	1GB personal and 1GB for Organizational items	1GB personal and 1GB for Organizational items
Bitwarden Authenticator	☑	☑
Vault Health Reports	☑	☑
Personal Emergency Access	☑	☑
Priority Support	☑	☑
Pricing	**$3/User/Month Get Started**	**$5/User/Month Get Started**

Kuva 5. Bitwardenin hinnat työkäytössä. (Bitwarden a)

4.3 Google Password Manager

Google Password Manager on Google Chrome -selaimeen sisäänrakennettu salasanahallintatyökalu, jolla voi hallita käyttäjätietoja sekä luoda vahvoja ja yksilöllisiä salasanoja. Google Password Managerin käyttö on ilmaista ja vaatii vain Google Chromen asentamisen toimiakseen. Kirjautumalla Google-tilille asetuksista voi määritellä salasanojen synkronoinnin päälle, jolloin tallennettuja käyttäjätietoja voi lisätä, poistaa tai muokata eri laitteilla Google Chromen kautta. Google Password Managerin ominaisuuksiin kuuluu automaattinen kirjautumistietojen täyttö sekä työkalu, joka ilmoittaa salasanojen laadukkuudesta. (Google)

5 VERTAILU

Vertailussa testataan ja tutkitaan tuotetta tai palvelua ja verrataan sitä toiseen, arvioiden niiden eroja. Tässä opinnäytetyössä vertaillaan kolmea salasanahallintaohjelmaa: KeePassXC:tä, ilmaisversiota Bitwardenista ja Google Password Manageria. Tässä kappaleessa tarkastellaan ja vertaillaan ohjelmien asennusta, käyttöä sekä turvallisuutta. Vertailuosuuden lopusta löytyy taulukko, jossa tähän opinnäytetyöhön valittuja salasanahallintaohjelmia vertaillaan ominaisuuksittain.

5.1 Asennus

Salasanahallintaohjelmaa käyttäessä ensimmäinen askel on ladata ohjelma valitulle alustalle ja asentaa se. Usein salasanahallintaohjelmien käyttöliittymät ovat hyvin samantyylisiä tietokone- ja mobiiliversioissa, joten ohjelman käyttöönottovaiheessa ja salasanoja määrittäessä on helpointa asentaa ja aloittaa käyttö ensin tietokoneversiolla tai selainlaajennuksella. Myöhemmin voi ladata mobiiliversion, mikäli sellainen on saatavilla, parantamaan käyttäjäkokemusta. Kaikkien kolmen vertailtavan salasanahallintaohjelman latauslinkit löytyvät suoraan ohjelmien omilta kotisivuilta.

Kaikkien kolmen ohjelman asentaminen on hyvin suoraviivaista: ne asennetaan samalla tavalla, kuin muutkin tavalliset päätelaitteilla käytettävät ohjelmat. KeePassXC:lle, Bitwardenille ja Google Password Managerille löytyy tuki yli 30 eri kielelle, suomi mukaan luettuna.

5.2 Käyttöönotto

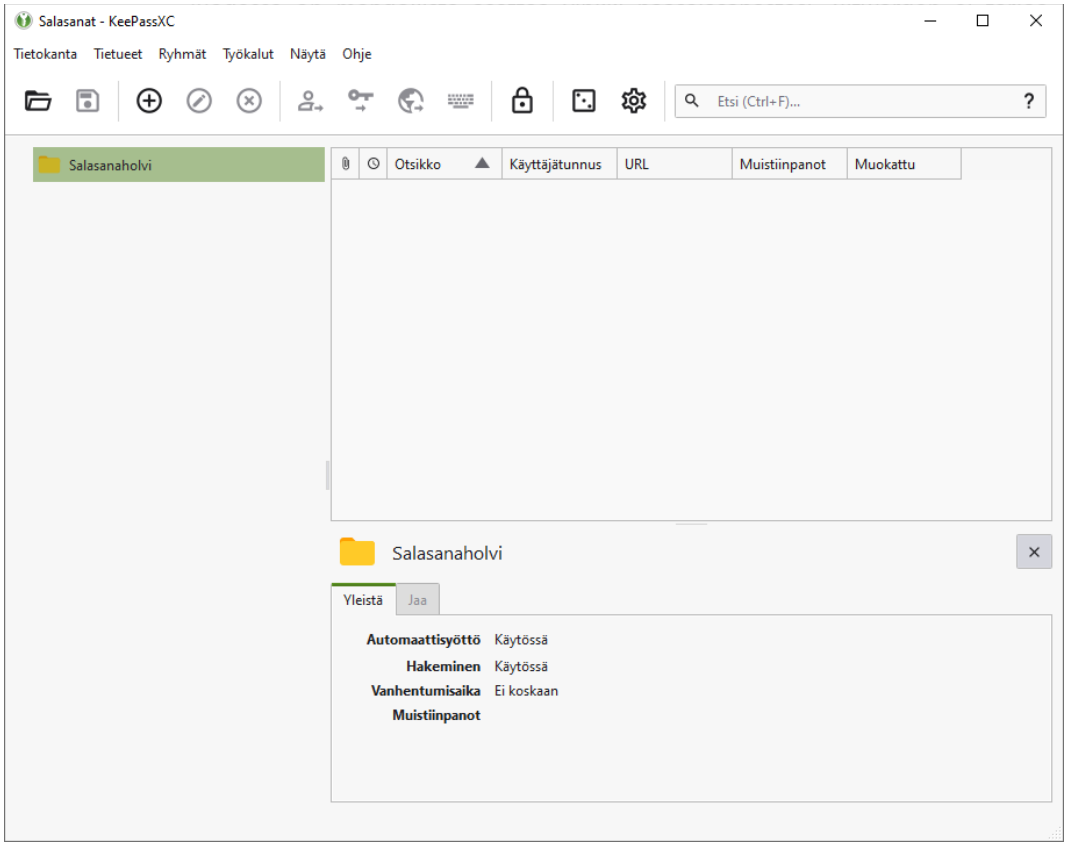
Joidenkin salasanahallintaohjelmien käyttöönotto edellyttää tilin luomista. Google Password Managerin ja KeePassXC:n tapauksessa tiliä ei ole pakko luoda, jotta ohjelmaa pystyy käyttämään. KeePassXC:een käyttöön ei tarvita tiliä laisinkaan, mutta vastaavasti Google Password Managerissa kirjautumatta jättäminen karsii ohjelman ominaisuuksia, kuten salasanan laadukkuuden testaustyökalun käytön,

salasanojen synkronoinnin useamman laitteen välillä, salasanaholvin varmuuskopioinnin tai pääsalasanan palautuksen sen unohtuessa.

Bitwardenin käyttö aloitetaan tekemällä tili ohjelman omalla kotisivulla. Tiliä tehdessä asetettu salasana toimii samalla salasanaholvin pääsalasanana, jolla pääsee hallinnoimaan salasanoja. Pääsalasanan on hyvä olla vahva ja mieleenpainuva, sillä jos joku ulkopuolinen pääsee kirjautumaan salasanaholviin, hänellä on pääsy jokaiseen salasanaan. Muistin virkistämiseksi Bitwarden-tiliä luodessa on mahdollista asettaa vinkki pääsalasanasta. KeePassXC on ainut ohjelmista, jossa ei ole pääsalasanan palautusominaisuutta, joten pääsalasanan unohtuessa pääsy salasanaholviin estyy kokonaan.

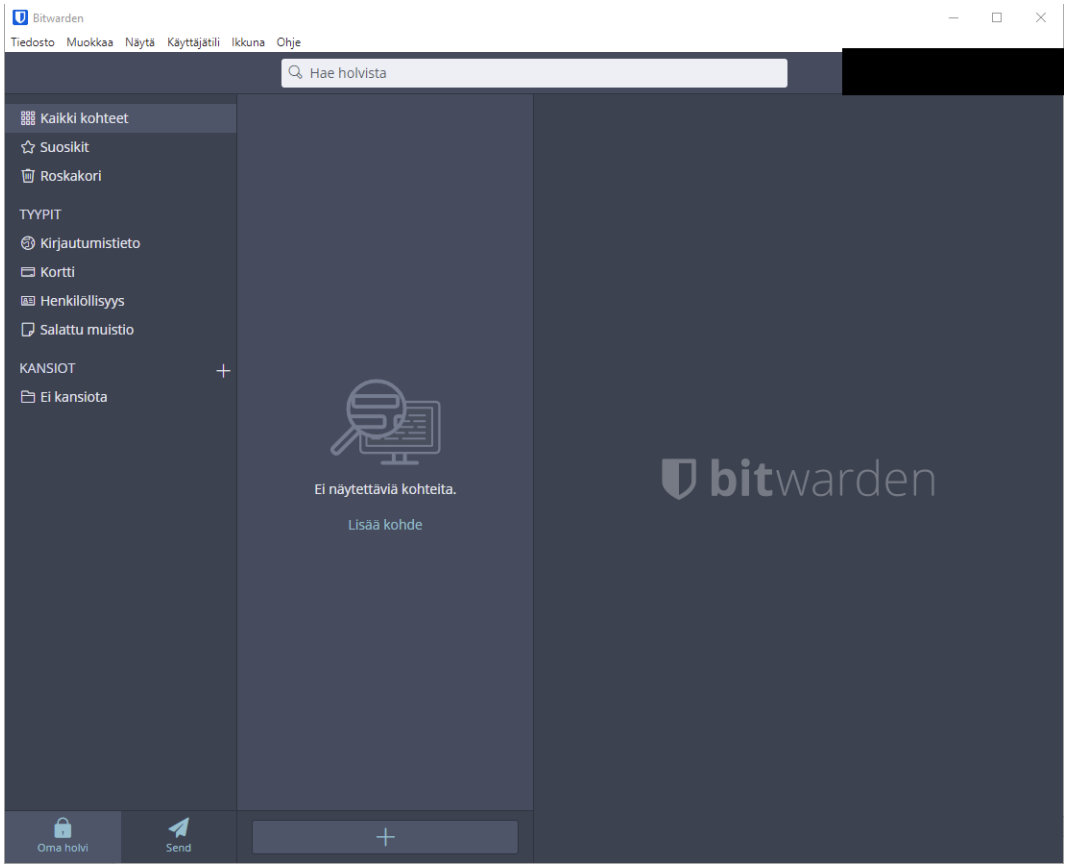
5.3 Salasanaholvin luominen

Salasanahallintaohjelmien salasanat tallennetaan salasanaholviin, joita pääsee hallinnoimaan antamalla pääsalasanan. Vertailtavista ohjelmista KeePassXC:ssä salasanaholvin luominen on ylivoimaisesti kaikkein monipuolisin muutaman lisäasetuksen johdosta, joilla voi muuttaa salasanaholvin salaustapaa tai tuoda lisäturvaa lisäämällä avaintiedosto, joka tarvitaan kirjautuessa pääsalasanan lisäksi. Salasanaholvin luonnin jälkeen avautuu näkymä tyhjästä salasanaholvista (kuva 6).



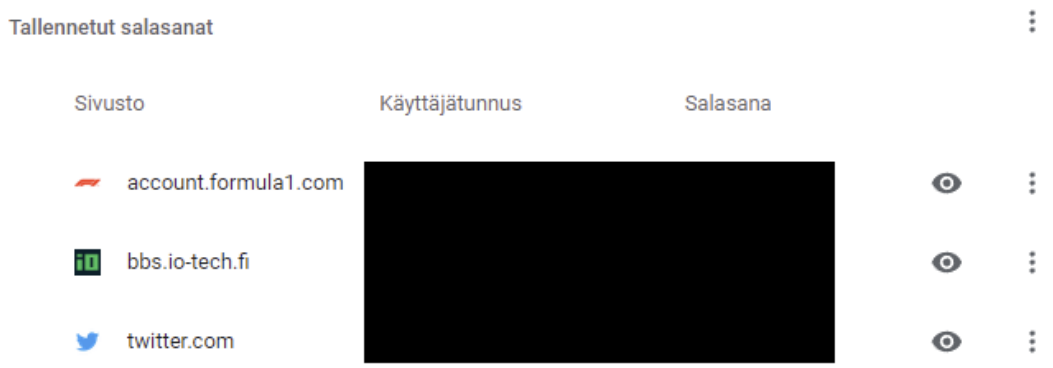
Kuva 6. KeePassXC:n aloitusnäkymä salasanaholvin luonnin jälkeen.

Bitwardenissa salasanaholvi luodaan samalla kun kirjautuu ensimmäistä kertaa ohjelmaan (kuva 7).



Kuva 7. Bitwarden aloitusnäkymä kirjautumisen jälkeen tietokoneversiossa.

Google Password Managerissa salasananholvin luominen tapahtuu automaattisesti, kun ottaa käyttöön salasanojen tallentamisen Chromen asetuksista ja tallentaa ensimmäisen salasanan holviin (kuva 8).



Kuva 8. Google Password Managerin salasanaholvi.

5.4 Salasanojen tuonti toisesta ohjelmasta

Useimmissa salasanahallintaohjelmissa on ominaisuus, jolla voi tuoda salasanat toisesta ohjelmasta. Salasanojen tuontityökalu helpottaa ja nopeuttaa salasanahallintaohjelman käyttöönottoa huomattavasti, kun ei tarvitse aloittaa täysin tyhjästä. Salasanahallintaohjelmasta riippuen tuontityökalu voi vaatia, että salasanat on tallennettu tietyssä tiedostomuodossa. Kaikkiin kolmeen vertailtavaan ohjelmaan salasanat voi tuoda tiedostosta, joka on tallennettu CSV-tiedostomuotoon. KeePassXC:ssä salasanojen tuonti onnistuu suoraan 1Password-ohjelmasta tai KeePass 1 -tietokannasta, kun Bitwardenissa tuontityökalu on kaikista kattavin, sillä tuki löytyy yli 30 eri salasanahallintaohjelmalle.

5.5 Salasanojen hallinnointi

Salasanahallintaohjelman asentamisen ja käyttöönoton jälkeen alkaa työläin vaihe ohjelman käytössä, kun aloitetaan salasanojen lisäys ja tallennus ohjelmaan. Olemassa olevien tilien salasanojen vahvuudesta riippuen on hyvä vaihtaa nykyiset salasanat turvallisimmaksi. Tätä helpottaakseen kaikista kolmesta vertailtavasta ohjelmasta löytyy salasanojen laadun testaukseen soveltuva työkalu, tosin Google Password Managerissa se vaatii Google-tilin toimiakseen. KeePassXC:n ja Bitwardenin tapauksessa selainlaajennuksen asentaminen

nopeuttaa käyttöä, kun kirjautumalla verkkopalveluihin laajennuksen avulla voi tallentaa kirjautumistiedot suoraan salasanaholviin. Monet salasanahallintaohjelmien selainlaajennukset osaavat ehdottaa vahvaa salasanaa uutta tiliä luodessa tai vanhaa salasanaa vaihtaessa, jolloin ohjelma tekee käyttäjän työn helpoksi. Kaikista kolmesta vertailtavasta ohjelmasta löytyy kyseinen ominaisuus, tosin Google Password Managerissa tämäkin ominaisuus vaatii Google-tilin toimiakseen. Salasanojen lisäyksen ja tallennuksen lisäksi salasanoja voi muokata ja poistaa holvista.

5.6 Kirjautuminen sivustoille

Asennuksen ja alun salasanojen määrittelyn jälkeen ohjelman käyttö on pääasiassa kirjautumista eri sivustoille salasanahallintaohjelmaa apuna käyttäen. Käyttäjätunnuksen ja salasanan voi kopioida salasanaholvista kirjautumissivulle tai käyttää automaattista täyttöä, joka lisää kirjautumistiedot suoraan kirjautumiskenttiin. Automaattinen täyttö löytyy kaikkien kolmen vertailtavien ohjelmien versioista lukuun ottamatta Bitwardenin työpöytäsovellusta ja verkkosivun kautta käytettävää salasanaholvia.

5.7 Turvallisuus

Salasanahallintaohjelmissa turvallisuus on yksityisyyden, verkkoturvallisuuden ja tietojen suojaamisen kannalta erittäin tärkeää, koska ohjelmat käsittelevät arkaluontoisia tietoja. Salasanahallintaohjelmista löytyy tietoturvaominaisuuksia, kuten kaksivaiheinen ja biometrinen tunnistus, joilla voi parantaa käyttäjän turvallisuutta. Kaikkiin kolmeen ohjelmaan voi asettaa kaksivaiheisen tunnistuksen, mutta vertailtavista ohjelmista ainoastaan KeePassXC ja Bitwarden tukevat salasanaholvin pika-avausta biometrisellä tunnistuksella.

Google Password Manager salaa synkronoidut salasanat Google-tilin avulla tai itse asetetulla synkronoinnin tunnuslauseella. Jos ohjelman salasanaholvin avaa ilman Google-tiliä, niin ohjelma pyytää käyttöjärjestelmän salasanaa tai mobiililaitteen

pin-koodia tai kuviota. Google ei kerro tarkemmin miten salasanaholvin tiedot salataan. Bitwarden ja KeePassXC salaavat salasanaholvit pääsalasanalla. Bitwardenissa salaus toteutetaan AES-256-algoritmilla. KeePassXC:ssä käytetään myös samaa algoritmia salaamiseen oletusasetuksella.

Google Password Manager sekä Bitwarden parantavat tietoturvaa teettämällä kolmannen osapuolen tietoturva-auditointeja.

5.8 Ominaisuustaulukko

Taulukossa 1 vertaillaan salasanahallintaohjelmia tärkeimpien ominaisuuksien perusteella.

Taulukko 1. Ominaisuustaulukko.

	KeePassXC	**Bitwarden**	**Google Password Manager**
Hinta	Ilmainen	Ilmainen, myös maksullisia versioita	Ilmainen
Tuetut alustat	Windows, MacOS, Linux	Windows, MacOS, Linux, iOS, Android, verkkosivusto	Google Chrome (Windows, MacOS, Linux, iOS, Android), verkkosivusto
Selainlaajennus	Chrome, Chromium, Vivaldi, Brave, Mozilla Firefox, Tor, Microsoft Edge	Chrome, Vivaldi, Brave, Mozilla Firefox, Tor, Microsoft Edge, Opera, Safari	Google Chrome
Asiakastuki	Ohjesivusto	Ohjesivusto, sähköpostituki, foorumit	Ohjesivusto
Salasanojen tuonti toisesta ohjelmasta	Kyllä	Kyllä	Kyllä
Salasanojen tallennusmenetelmä	Paikallinen (vapaavalintainen pilvitallennus mahdollista)	Pilvitallennus	Paikallinen sekä pilvitallennus
Kaksivaiheinen tunnistus	Kyllä	Kyllä	Kyllä (vaatii Google-tilin)
Pääsalasanan palautus	Ei	Kyllä (vaatii maksullisen version)	Kyllä (vaatii Google-tilin)
Offline-käyttö	Kyllä	Kyllä (vain lukutila)	Kyllä
Salasanan laadukkuuden testaustyökalu	Kyllä	Kyllä	Kyllä (vaatii Google-tilin)

6 TULOKSET JA POHDINTA

Salasanat eivät ole ikinä täysin turvallisia, mutta salasanojen hallinnointiin käytetyt salasanahallintaohjelmat parantavat merkittävästi turvallisuutta. Salasanahallintaohjelmiin sisäänrakennetut salasanageneraattorit osaavat luoda tarpeeksi pitkiä ja vahvoja salasanoja. Ohjelmien avulla on helppo luoda tilikohtaisia salasanoja, kun tyypillisesti käytetään uudelleen samoja salasanoja eri verkkopalveluissa. Yksi salasanahallintaohjelmien pääteemoista on se, että tarvitsee muistaa vain yksi pääsalasana, jolla pääsee hallinnoimaan ohjelmaan tallennettuja salasanoja. Samalla se on myös salasanahallintaohjelmien isoin turvallisuusriski ja ongelma, kun kaikki tiedot ovat yhden pääsalasanan takana. Pääsalasanan vuotaessa huijarilla on pääsy jokaiseen salasanaan. Omaa turvallisuutta on mahdollista parantaa ottamalla käyttöön ohjelmien tarjoamia ominaisuuksia, kuten kaksivaiheisen tunnistuksen.

Pääsalasana voi olla hyvä kirjoittaa esimerkiksi paperille ja pitää sitä jossain turvallisessa paikassa tallessa. Muutoin pääsalasanan unohtuessa joutuu käyttäjä uusimaan kaikki salasanansa, mikäli salasanahallintaohjelmassa ei ole pääsalasanan palautusominaisuutta. Salasanahallintaohjelmaa valitessa onkin hyvä tarkastella mitä ominaisuuksia se tarjoaa ja tehdä valintapäätös niiden perusteella. Ensimmäisenä valintakriteerinä voidaan pitää salasanojen tallennusmenetelmää, eli tallennetaanko ne paikallisesti käytetylle päätelaitteelle vai palveluntarjoajan pilvipalvelimille. Pilvipalvelupohjaisten ohjelmien etuna salasanat kulkevat kätevästi mukana, jolloin ohjelman käyttö onnistuu käytännössä missä tahansa. Kuitenkin mikäli pilvipalvelin joutuu tietomurron kohteeksi, on hakkereilla pääsy holvin salattuihin tietoihin. Toinen heikkous on se, että jos palvelimet kaatuvat hetkeksi tai ne suljetaan kokonaan, estyy pääsy salasanoihin, mikäli ohjelmassa ei ole mahdollisuutta offline-käyttöön. Palvelinten ollessa pois käytöstä on tärkeää, että offline-toiminnallisuus löytyy, jolloin käyttäjä voi jatkaa ohjelman käyttöä ja mahdollisesti siirtää tallennetut salasanat toiseen ohjelmaan. Paikalliseen tallennukseen perustuvat salasanahallintaohjelmat eivät

ole yhtä käytännöllisiä verrattuna pilvipalvelupohjaisiin, kun tallennetut salasanat on sidotut käytettyyn laitteeseen. Salasanaholvin varmuuskopiointi sekä synkronointi eri laitteiden välillä on työlästä, kun sen joutuu tekemään manuaalisesti. Paikalliseen tallennukseen perustuvia salasanahallintaohjelmia voidaan kuitenkin pitää turvallisempana olettaen, että on vaikeampaa murtautua paikallisesti tallennettuun salasanaholviin kuin palvelimelle tallennettuun.

Toisena valintakriteerinä voidaan pitää salasanahallintaohjelmien alustatukea. Ohjelmista on tarjolla monia vaihtoehtoja ilmaisista maksullisiin: tietokoneille, mobiililaitteille, eri selaimille tai suoraan verkkosivuston kautta käytettäviä. On hyvä kartoittaa omat käyttötarpeet, missä ja milloin tarvitsee salasanoja ja tehdä ohjelman valinta sen perusteella. Valinnan viimeistelevät salasanahallintaohjelman lisäominaisuudet ja se, onko valmis maksamaan ohjelman käytöstä vai onko olemassa ilmaisia ohjelmia, joiden ominaisuudet riittävät omiin käyttötarpeisiin.

KeePassXC on avoimen lähdekoodin ohjelma, jonka ainoa tulonlähde on vapaaehtoiset lahjoitukset käyttäjiltä. Uusia ominaisuuksia tai päivityksiä ei tule välttämättä samalla tahdilla kuin kaupallisiin ohjelmiin. Salasanaholvin varmuuskopioinnista ja synkronoinnista eri laitteiden välillä pitää huolehtia itse jos käyttää salasanahallintaohjelmaa, jossa salasanaholvi tallennetaan paikallisesti, kuten KeePassXC:ssä. KeePassXC:stä puuttuu pääsalasanan resetointi, joten pääsy salasanoihin estyy kokonaan, mikäli käyttäjä unohtaa pääsalasanan. KeePassXC:stä ei ole saatavilla omia versioita mobiililaitteille, mutta mobiililaitteille löytyy kuitenkin ohjelmia, jotka tukevat KeePassXC:ssä luotuja salasanaholveja. Säädettävyydeltään KeePassXC on kolmesta vertailtavasta ohjelmasta monipuolisin, mutta samalla asetusten suuri määrä voi heikentää käytettävyyttä käyttäjästä riippuen.

Bitwardenin alustatuki on kaikkein kattavin vertailtavista ohjelmista, kun ohjelma toimii käytännössä jokaisella nykypäivän laitteella. Salasanaholvi on tallennettu Bitwardenin omalle palvelimille, jolloin synkronoidut salasanat kulkevat mukana

tilanteen mukaan. Myös tietojen tallennus itse pystytetylle palvelimelle onnistuu, mikäli haluaa täyden kontrollin tietoihin. Bitwardenin ilmaisversiota käytettäessä on syytä huomioida, että pääsalasanan resetointi on maksumuurin takana.

Google Password Managerin käyttö ilman Google-tiliä rajoittaa roimasti ohjelmassa saatavilla olevia ominaisuuksia. Google Password Managerin käyttö vaatii toimiakseen Google Chromen, joten käyttäjä on lukittu yhteen selaimeen. Selaimiin sisäänrakennetut salasanahallintaohjelmat toimivat vain yhdellä tietyllä selaimella. Jos käyttäjä vaihtaa eri selaimeen, eivät selaimet tue keskenään salasanojen synkronointia, vaan kaikki salasanat joutuu siirtämään selaimesta toiseen manuaalisesti. Google Password Manager ei ole avoimen lähdekoodin ohjelma, joten käyttäjä joutuu luottamaan Googlen tapaan toimia.

Yksiselitteisesti on vaikea todeta mikä vertailtavista ohjelmista on paras. Se mikä ohjelma sopii käyttäjälle parhaiten riippuu käyttäjän vaatimuksista ja tarpeista. Jos haluaa pitää salasanat täysin omassa hallinnassaan ja turvata itse yksityiset tiedot, on KeePassXC tällöin paras. Bitwarden on hyvä valinta, jos tarvitsee pääsyn salasanoihin eri alustoilla. Google Password Manager on kahdesta muusta vertailtavasta ohjelmasta poikkeus siten, että se on erillinen työkalu selaimessa eikä itsenäinen salasanojen hallinnointiin tehty ohjelma. Google on suunnittelut työkalusta pelkistetyn mikä tekee siitä vertailtavista ohjelmista helppokäyttöisimmän.

Opinnäytetyön alussa asetetut tavoitteet saavutettiin. joten työhön voi olla tyytyväinen. Aiheesta voisi tehdä jatkotutkimusta esimerkiksi ottamalla vertailuun mukaan maksullisia salasanahallintaohjelmia.

LÄHTEET

Bacon, M. 2021. Password. Viitattu 22.1.2022. https://www.techtarget.com/searchsecurity/definition/password

Bitwarden a. Bitwarden Plans and Pricing. Viitattu 23.4.2022. https://bitwarden.com/pricing/business/

Bitwarden b. Bitwarden Plans and Pricing. Viitattu 23.4.2022. https://bitwarden.com/pricing/

Bitwarden c. Products. Viitattu 18.4.2022. https://bitwarden.com/products/

Cisco. What Is Encryption? Viitattu 9.4.2022. https://www.cisco.com/c/en/us/products/security/encryption-explained.html#~encryption-algorithms

Druva. What is data encryption definition and related faqs. Viitattu 9.4.2022. https://www.druva.com/glossary/what-is-data-encryption-definition-and-related-faqs/

Encryption consulting. What is the difference between Symmetric and Asymmetric Encryption? Which is better for data security? Viitattu 20.4.2022. https://www.encryptionconsulting.com/education-center/symmetric-vs-asymmetric-encryption/

F-Secure. Miten käyttäjätilin kaappaus tapahtuu? Viitattu 5.2.2022. https://www.f-secure.com/fi/home/articles/how-account-takeover-happens

Gibbs, S. 2016. Passwords and hacking: the jargon of hashing, salting and SHA-2 explained. Viitattu 6.3.2022. https://www.theguardian.com/technology/2016/dec/15/passwords-hacking-hashing-salting-sha-2

Google 2019. Online Security Survey. Viitattu 3.5.2022. https://services.google.com/fh/files/blogs/google_security_infographic.pdf

Google. Salasanojen tallentaminen, ylläpitäminen ja suojaaminen. Viitattu 18.4.2022. https://support.google.com/accounts/answer/6208650?hl=fi

Hougen, A. 2021. What Is AES Encryption & How Does It Work in 2022? 256-bit vs 128-bit. Viitattu 27.4.2022. https://www.cloudwards.net/what-is-aes/

Kaspersky. Brute Force Attack: Definition and Examples. Viitattu 23.1.2022. https://www.kaspersky.com/resource-center/definitions/brute-force-attack

KeePassXC. Project. Viitattu 17.4.2022. https://keepassxc.org/project/

Kyberturvallisuuskeskus 2021a. Neuvoja salasanan hallintasovelluksen käyttöönottoon. Viitattu 19.4.2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon

Kyberturvallisuuskeskus 2021b. Sähköinen tunnistaminen. Viitattu 29.1.2022. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen

Kyberturvallisuuskeskus. Salasanat haltuun - Neuvoja salasanojen käyttöön ja hallintaan. Viitattu 22.1.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Salasanat_haltuun.pdf

Lake, J. 2022. What is SHA-2 and how does it work? Viitattu 19.4.2022. https://www.comparitech.com/blog/information-security/what-is-sha-2-how-does-it-work/

Lehto, V. 2021. Miksi käytämme salasanoja tunnistautumiseen? Viitattu 29.1.2022. https://bluugo.fi/blog/miksi-kaytamme-salasanoja-tunnistautumiseen/

Mezquita, T. 2020. Password Salting. Viitattu 23.1.2022. https://cyberhoot.com/cybrary/password-salting/

Mikrobitti 2020. Mikä on VPN? Viitattu 28.2.2022. https://www.mikrobitti.fi/neuvot/mika-on-vpn/61708851-881b-435a-ab31-4164c58eaa69

Signicat 2021. Vahva sähköinen tunnistaminen ja tunnistautuminen. Viitattu 29.1.2022. https://www.signicat.com/fi/blogi/vahva-s%C3%A4hk%C3%B6inen-tunnistaminen-ja-tunnistautuminen

STEK. Tietojen suojaaminen ja tunnistaminen. Viitattu 29.1.2022. https://stek.fi/termit/autentikointi

Swinhoe, D. 2020. What is a dictionary attack? And how you can easily stop them. Viitattu 26.3.2022. https://www.csoonline.com/article/3568794/what-is-a-dictionary-attack-and-how-you-can-easily-stop-them.html

Tarsnap. Scrypt. Viitattu 9.3.2022. https://www.tarsnap.com/scrypt.html

Welekwe, A. 2022. What is a Rainbow Table Attack? Viitattu 27.3.2022. https://www.comparitech.com/net-admin/rainbow-table-attack/