FIDO2 käytettävyys ja käyttökelpoisuus

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tietotekniikka
Toukokuu 2024
Topias Kinnunen

TURUN YLIOPISTO
Tietotekniikan laitos

Topias Kinnunen: FIDO2 käytettävyys ja käyttökelpoisuus

TkK-tutkielma, 20 s.
Tietotekniikka
Toukokuu 2024

Salasanojen mahdollinen korvaaja FIDO2 on standardi, jolla on hyötyjä salasanatunnistautumiseen verrattuna, mutta myös haittoja. Tässä kirjallisuuskatsauksessa tutkitaan, mitä nämä hyödyt ja haitat ovat, miten ne vaikuttavat FIDO2:n käytettävyyteen ja käyttökelpoisuuteen ja pohditaan voiko FIDO2 korvata salasanatunnistautumisen. Ensin kuvataan salasanoista johtuvat heikkoudet ja syvennytään FIDO2:n toimintaan, jotta voidaan paremmin ymmärtää, mikä FIDO2:n rooli nykymaailmassa on ja mikä se voisi tulevaisuudessa olla. FIDO2:n käytettävyyden ongelmia katsotaan useista näkökulmista, niin teoreettisista, kuin konkreettisista. Tutkielmassa pohditaan ratkaisuja näihin käytettävyyteen liittyviin ongelmiin kirjallisuuskatsauksen avulla. Päätelmiä ja perusteluita on kerätty mm. monista käyttäjäkyselyistä sekä loogisista päätelmistä. Kirjallisuuskatsauksen lopussa vastataan tutkielman tutkimuskysymyksiin aiempien havaintojen ja omien pohdintojen pohjalta. Päädytään lopputulokseen, ettei FIDO2 ole vielä valmis mittavaan käyttöönottoon yritysten toimesta, mutta että se paranee hitaan käyttöönoton myötä. Yksityishenkilöiden käyttöönotto on kuitenkin jo paremmassa tilanteessa laajemman tuen takia, mutta suurin osa käyttäjistä ei vielä ole valmiita luopumaan salasanatunnistautumisesta.

Asiasanat: FIDO2, käytettävyys, käyttökelpoisuus, tunnistautuminen, todennus, salasana

Sisällys

1 Johdanto **1**

1.1 Taustaa 1

1.2 Tutkimuskysymys 2

1.3 Tiedonhaku 2

1.4 Tutkielman rakenne 3

2 FIDO2 ja siihen liittyvät ongelmat **4**

2.1 Miten FIDO2 toimii 4

2.2 FIDO2:n haasteet 8

3 Ongelmakohtien ratkaiseminen **10**

3.1 Palveluntarjoajien FIDO2 adoptio 10

3.2 FIDO2 tunnettavuus 11

3.3 Laajempi laitevalikoima ja tuki 11

3.4 Luottamuksen kasvattaminen 12

3.5 Käytettävyyden korjaaminen 13

4 FIDO2 käyttöönoton tulevaisuus **14**

4.1 Yksityisten henkilöiden FIDO2 käyttö 14

4.2 Yritysten FIDO2 käyttö 16

5 Yhteenveto **19**

Lähdeluettelo **21**

Kuvat

2.1 Epäsymmetrineseen salaukseen pohjautuva tunnistautuminen 5
2.2 Esimerkki FIDO2 toiminnasta 6
2.3 Passkey malli, perustuu FIDO:n malliin. [4] 7

1 Johdanto

1.1 Taustaa

FIDO2 on FIDO-liittouman (Fast Identity Online) salasanaton tunnistautumismenetelmä, joka pyrkii korvaamaan salasanatunnistautumisen. [1] Se käyttää W3C:n (World Wide Web Consortium) WebAuthn (Web Authentication) -spesifikaatiota ja FIDO-liittouman CTAP:tä (Client-to-Authenticator Protocol) tunnistautumisen taustalla. Sen salasanattomuus pyrkii korjaamaan salasanatunnistautumiseen liittyviä haasteita, kuten yhä yleistyvämmät kalastelusivut sekä salasanojen helpon unohtuvuuden. FIDO2 ei kuitenkaan ole täysin ongelmaton ratkaisu. FIDO2:n kohdalla nämä uudet ongelmat koskevat käytettävyyttä ja käyttökelpoisuutta.

Salasanapohjainen tunnistautuminen on yleisin tunnistautumismenetelmä nykypäivänä, tämän myötä se on myös suuri kohde kyberrikollisille. Salasanapohjaisen tunnistautumisen murtamiseksi on kehitetty vuosikymmenien aikana monia työkaluja, jotka käyttävät hyväksi salasanojen heikkouksia. Monet käyttäjät käyttävät usein samoja salasanoja useissa eri palveluissa, usein saman käyttäjänimen tai sähköpostitilin kanssa. Tämä lisää salasanan vuotamisen riskiä ja vuotamisesta aiheutuvan vahingon suuruutta. Salasanat voivat vuotaa huonosti suojattujen palveluiden kautta, jotka säilövät salasanaa turvattomasti, tai haittaohjelmassa olevan näppäilyntallentajan kautta.

Vuotaneita salasanoja käytetään myös hyväksi väsytyshyökkäyksien parantami-

sessa. Väsytyshyökkäykset käyttävät yleisimpiä salasanoja hyväksi tunnistautumisen rikkomisessa. Salasanakalastelu on viime vuosien aikana yleistynyt nopeasti [2], ja se on yksi suurimmista uhista salasanapohjaiselle tunnistautumiselle. Turvalliset salasanat ovat monimutkaisia ja siten myös helppoja unohtaa. Unohtamisen riskiä voi pienentää käyttämällä salasananhallintaohjelmaa, joka on vahvan salasanan takana. Tämä ei kuitenkaan poista riskiä unohtaa salasananhallintaohjelman salasana. Etuna FIDO2-tunnistautumisessa verrattuna salasanatunnistautumiseen on, ettei se ole altis kalasteluhyökkäyksille eikä tarvitse muistaa salasanaa.

Tässä kirjallisuuskatsauksessa tutkitaan, mitä ongelmia perinteisillä salasanapohjaisilla tunnistautumismenetelmillä on, mikä FIDO2 on, miten se ratkaisee nämä ongelmat ja mitä uusia ongelmia FIDO2:n toteutustavasta seuraa.

1.2 Tutkimuskysymys

Tutkielman päätutkimuskysymys on “mitkä asiat vaikuttavat FIDO2:n käytön helppouteen tai vaikeuteen.” Tämän kysymyksen rinnalla esitetään myös kaksi muuta tutkimuskysymystä, jotka ovat "voiko FIDO2 korvata salasanat"ja "miltä näyttää FIDO2:n tulevaisuus."Nämä tutkimuskysymykset pyrkivät tukemaan toisiaan ja ne vastaavat toisiinsa osittain.

1.3 Tiedonhaku

Tiedonhaku alkoi yksinkertaisella Google Scholar -haulla hakusanalla "FIDO2", joka tuotti 888 tulosta. Sopivamman määrän tuloksia sai tekemällä täsmennettyjä hakuja digitaalisesta ACM (Association for Computing Machinery) -kirjastosta, Springer Linkistä ja IEEEXploresta. Hakulausekkeena käytettiin "FIDO2 AND (’User Experience’ OR Usability*) AND Security", jolla hakutuloksia löytyi kirjastosta riippuen 8-32, joista lähteiksi valikoitui alustavasti 12. Hakulausekkeena kokeiltiin myös "FI-

DO2 AND ('FUTURE' OR 'ADOPTION')", jolla hakutuloksia löytyi kirjastosta riippuen 6-32. Useat näistä hakutuloksista löytyi aiemmalla hakulausekkeella, eikä yhtäkään uutta sopivaa lähdettä löytynyt uudella hakulausekkeella.

Hakulausekkeiden muodostamisessa käytettiin hyväksi ChatGPT:tä. Sille annettiin alustavaksi tiedoksi tutkimuskysymykset ja muutamia aiheeseen liittyviä hakusanoja ja sitä pyydettiin generoimaan lisää samanlaisia hakusanoja. ChatGPT generoi paljon hyvin yleislaatuisia sanoja, jotka eivät sopineet hakusanoiksi tai eivät liittyneet aiheeseen. Generoituneiden hakusanojen joukosta löytyi kuitenkin muutamia hyväksyttäviä hakusanoja, kuten "usability study"ja "user experience", joiden avulla ensimmäinen hakulauseke muodostettiin. Samaa menetelmää käytettiin toisen hakulausekkeen hakusanojen generoimiseen, mutta mikään niistä ei sopinut hakusanaksi.

Lähteeksi valikoitui pääasiassa FIDO2:n käytettävyyteen liittyviä artikkeleita, tutkimusartikkeleita ja konferenssijulkaisuja. Lähteenä käytettiin myös FIDO-liittouman omia teknisiä dokumentaatioita, sekä käyttöönottokokemuksia mm. Googlelta.

1.4 Tutkielman rakenne

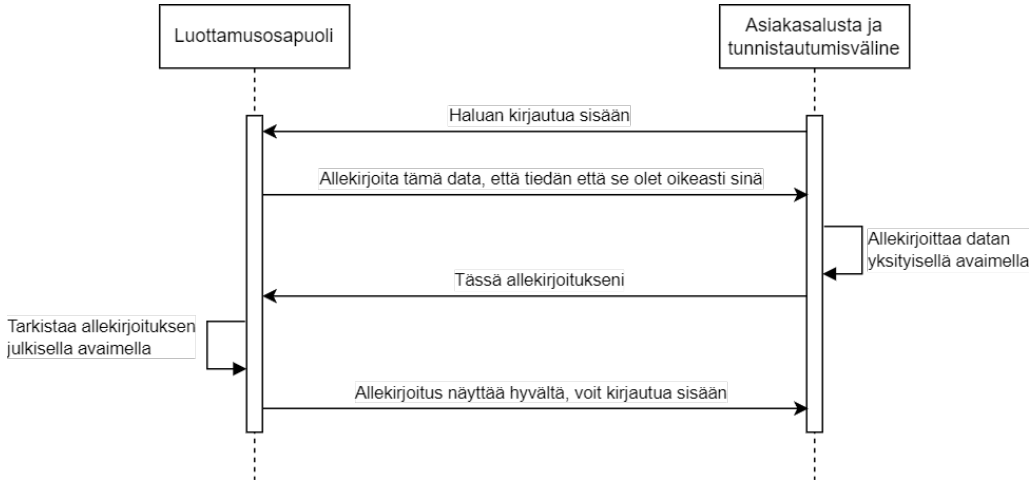
Tutkielman toisessa luvussa käsitellään FIDO2:ta ja siihen liittyviä ongelmia. Siinä selitetään myös FIDO2:n toimintaperiaatteita. Kolmannessa luvussa käsitellään, miten FIDO2 ongelmia voitaisiin helpottaa ja syvennytään sen myötä ongelmien syihin. Neljännessä luvussa analysoidaan FIDO2:n tulevaisuuden näkymiä ja sen mahdollisuuksia toimia salasanapohjaisen tunnistautumismenetelmän korvaajana yksityishenkilöillä sekä yritystoiminnassa. Viidennessä luvussa kerätään aiempien kappaleiden päätelmiä kasaan ja tehdään näiden pohjalta johtopäätöksiä, yritetään vastata tutkimuskysymyksiin ja tehdään yhteenveto.

2 FIDO2 ja siihen liittyvät ongelmat

2.1 Miten FIDO2 toimii

FIDO2-tunnistautuminen pohjautuu julkisen avaimen salaukseen. Yksityistä avainta säilytetään tunnistautumislaitteella, jonka avulla pystytään tunnistautumaan haluttuun palveluun allekirjoittamalla palvelun lähettämä haaste. Tunnistautumiseen voidaan käyttää laitetta, jolla palvelun käyttäminen tapahtuu tai voidaan käyttää ulkoista laitetta, joka toimii vain tunnistimena. Perinteinen salasanatunnistautuminen perustuu tunnistautuvan osapuolen tietämään asiaan – salasanaan. Vastaavasti FIDO2-tunnistautumisessa käytetään jotain, mitä tunnistettava on, omistaa tai tietää. Tämä asia voi olla sormenjälki, kuva iiriksestä, elektroninen henkilökortti, USB-turva-avain tai pin-koodi.

WebAuthn [3] on spesifikaatio, johon FIDO2 perustuu. WebAuthn käyttää hyväkseen julkisen avaimen salausta, jossa julkinen avain annetaan palvelulle, johon kirjaudutaan ja yksityinen avain säilytetään tunnistautumislaitteessa. Jokaiselle palvelulle on oma avainpari ja todistus tunnistautumislaitteesta. Todistus auttaa tilanteissa, joissa avainparin yksityinen avain on vuotanut, koska palvelu voi vaatia todistuksen, joka on vain tunnistautumislaitteella. Monikaan palvelu ei kuitenkaan käytä tätä todistusta. CTAP on toinen protokolla, jonka avulla FIDO2 toimii. Tämän protokollan avulla tunnistautumislaite ja tunnistautumista vaativa palvelu pystyvät kommunikoimaan keskenään. FIDO2 käyttää CTAP:n versiota 2.

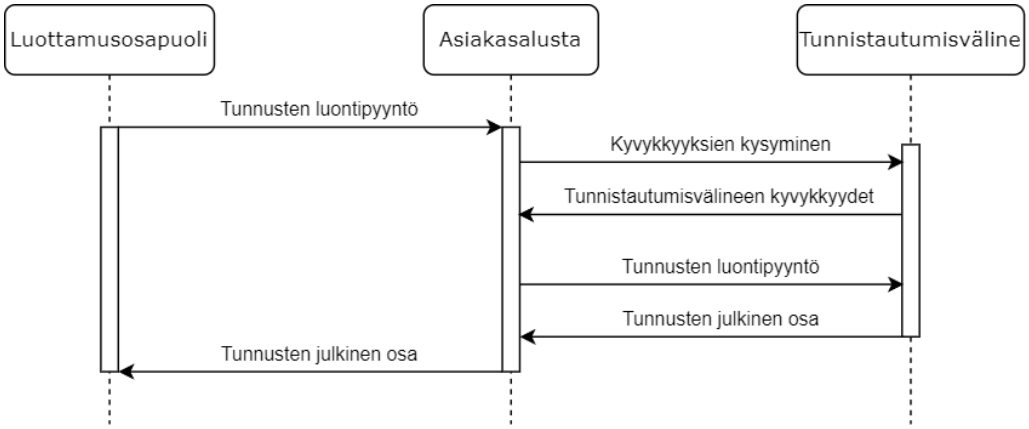


Kuva 2.1: Epäsymmetrineseen salaukseen pohjautuva tunnistautuminen

Kuvassa 2.1 näytetään, miten epäsymmetrinen salaus toimii WebAuthn:ssa. Tyypillisesti epäsymmetristä salausta käytetään sertifikaateissa. Sertifikaatin avulla verkkosivu voi todistaa olevansa se verkkosivu, joka väittää olevansa. WebAuthn:ssa todistavana osapuolena on asiakas-palvelin-arkitehtuurin asiakas. Tällöin asiakas todistaa olevansa tilin omistaja allekirjoittamalla palvelimen lähettämän haasteen.

Epäsymmetrisessä salauksessa luottamusosapuoli – eli palvelin – antaa dataa tai "haasteen", jonka asiakas allekirjoittaa tai salaa yksityisellä avaimellaan. Allekirjoitettu data lähetetään takaisin luottamusosapuolelle, joka purkaa epäsymmetrisen salauksen julkisella avaimella. Datan palautuessa alkuperäiseen muotoonsa voidaan todeta, että asiakas on kuka väittää olevansa. Kirjautuminen voidaan hylätä, mikäli data ei palaudu alkuperäiseen muotoonsa salauksen purkamisen jälkeen.

Kuvassa 2.2 on yksi esimerkki FIDO2:n toiminnasta. Tunnusten luontipyynnön paikalla voisi olla mikä tahansa CTAP:n tukema pyyntö. Luottamusosapuoli – joka voi olla verkkosivu tai muu palvelu – toimii tämän vuorovaikutuksen aloittajana. Luottamusosapuoli on palvelu, joka tarvitsee tunnistautumista käyttäjiltä. Asiakasalusta on palveluun tunnistautuessa käytettävä asiakaslaite. Luottamusosapuolen lähettäessä tunnistautumispyynnön – käyttäen FIDO2 protokollaa – asiakasalusta käsittelee pyynnön ja käyttää paikallisesti säilytettäviä tietoja tunnistautumisväli-

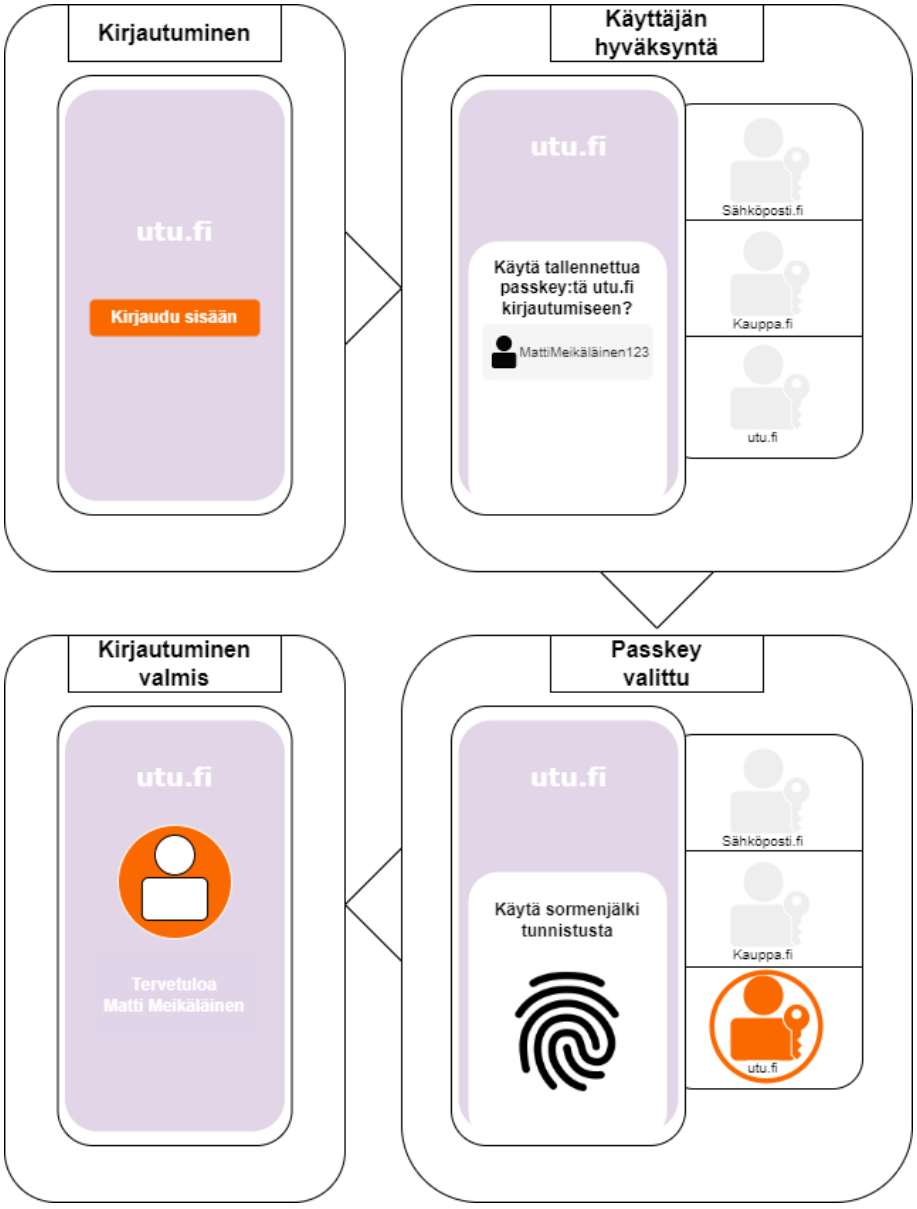


Kuva 2.2: Esimerkki FIDO2 toiminnasta

neen määrittämiseksi. Tilin luomisessa asiakasalusta ohjaa epäsymmetrisen salauksen julkisen avaimen luottamusosapuolelle. [3]

Asiakasalustan ja tunnistautumisvälineen välinen viestintä toimii CTAP:lla. Viestinnän väylänä voidaan käyttää langattomia yhteyksiä kuten Bluetooth tai NFC (Near Field Communication), tai langallisia yhteyksiä kuten USB-väylää. Asiakasalusta tekee tarvittavat kyselyt tunnistautumisvälineen ominaisuuksista, määrittääkseen miten tunnistautuminen suoritetaan. Kun asiakasalustalla on kaikki tarvittavat tiedot tunnistautumisvälineestä, se välittää luottamusosapuolen pyynnön ja asiakasalustalla säilytetyt tarvittavat tiedot tunnistautumisvälineelle. Tunnistautumisväline käsittelee pyynnön ja antaa vastauksen. Tunnistautumisvälineen vastaus riippuu pyynnön tarkoituksesta. Tunnusten luontipyynnön tapauksessa vastaus on joko tunnusten julkinen osa tai virhe.[3]

Passkeyt ovat FIDO2:n avainpareja, jotka korvaavat salasanakirjautumisen. Perinteisen salasanan sijasta käyttäjä rekisteröityy PIN-koodin tai biometrisen tunnisteen avulla. Kun käyttäjä haluaa myöhemmin kirjautua tilille, jonka on rekisteröinyt, hän hyväksyy kirjautumisen rekisteröitymiseen käytetyllä laitteellaan samalla tunnistautumisen menetelmällä kuin aiemmin. Tämä tarkoittaa, että jos käyttäjä on luonut passkeyn biometrista tunnistusta käyttäen, hän myös kirjautuu jatkossa biometrista tunnistusta käyttäen. [4]



Kuva 2.3: Passkey malli, perustuu FIDO:n malliin. [4]

Passkey-mallia esittävässä kuvassa 2.3 esitetään kirjautumisprosessi alusta loppuun. Sisäänkirjautumisen alussa palvelu lähettää käyttäjän laitteeseen haasteen, jonka käyttäjälaite tai ulkoinenen tunnistautumislaite salaa valittavan passkeyn salaisella avaimella. Valitaan Passkey-tunnus, jolla halutaan kirjautua. Yhdellä käyttäjällä voi olla useampi Passkey-tunnus yhtä palvelua varten, sekä muita tunnuksia muita palveluita varten. Paskkey-tunnusta käytettäessä käyttäjän täytyy tunnistau-

tua pin-koodilla tai biometrisellä tunnisteella, jotta varmistetaan käyttäjän olevan tilin omistaja. Kun käyttäjä on tunnistautunut, tunnistautumislaite salaa haasteen ja lähettää sen palvelulle käyttäjätunnisteen kanssa. Tunnistautumislaitteen ollessa ulkoinen, tunnistelaite lähettää salatun haasteen takaisin kirjautumislaitteelle, joka lähettää sen eteenpäin kirjauduttavaan palveluun. [4]

Rekisteröityminen palveluun tapahtuu niin, että käyttäjä lähettää rekisteröitymispyynnön palvelulle, jossa palvelulle annetaan epäsymmetrisen salauksen julkinen avain ja käyttäjätunnus. Julkinen avain ja käyttäjätunnus on verrannollinen salasanaan ja käyttäjänimeen toiminnallisuuden kannalta. Näiden suurin ero on, että julkisen avaimen – jolla salasana korvataan – vuotaminen ei ole yhtä suuri tietoturvariski, kuin salasanan vuotaminen salauksen epäsymmetrisyyden vuoksi. Palvelu tietää, mitä julkista avainta tulee käyttää haasteen salauksen purkamiseen käyttämällä saamaansa pyynnön mukana tullutta käyttäjätunnusta.

2.2 FIDO2:n haasteet

FIDO2:n käyttö ei ole tällä hetkellä yleistä. Osa syytä on palveluntarjoajien puutteellinen tuki. FIDO-liittouman jäseninä on kuitenkin monia suuria yrityksiä – kuten Google ja Microsoft – joista monet muut teknologiayritykset ottavat mallia. Tällä hetkellä Google tarjoaa mahdollisuuden käyttää FIDO2:ta ensisijaisena kirjautumismenetelmänä yksityis- ja yritys- Google-tileille [5]. Myös Microsoft tukee FIDO2:n käyttöä palveluissaan vaihtelevasti. Vaikka FIDO2:n adoptio on kiihtynyt yleisesti ottaen, monet palvelut eivät siltikään tarjoa mahdollisuutta tunnistautua FIDO2:n avulla.

Tunnistautuminen FIDO2:n avulla vaatii laitteita, joilla on tiettyjä ominaisuuksia. Laitteena voivat toimia mm. puhelin tai USB-turva-avain. Tämä asettaa esteen käyttäjän ja FIDO2:n väliin, sillä kaikilla ei välttämättä ole laitteita, jotka tukevat FIDO2:n käyttöä. Vaikka FIDO2 tukee kirjautumislaitteella tunnistautumista, se

vaatii TPM:n (Trusted Platform Module), jota kaikissa laitteissa ei ole. TPM toimii todentajana ulkoisen todentajalaitteen sijaan. Kaikki käyttäjät eivät ole tietoisia, tukeeko heidän laitteensa FIDO2:ta. [6]

Vaikka käyttäjillä olisikin sopivat laitteet FIDO2-tunnistautumisen käyttämiseksi ja palveluntarjoajat tukisivat tätä tunnistautumisen muotoa, voi silti olla, ettei käyttäjä luota salasanattomaan tunnistautumiseen [7]. Monet käyttäjät ovat myös tottuneet käyttämään salasanoja, eivätkä halua vaihtaa tuntemattomaan menetelmään. Vieras tunnistautumismenetelmä voi tuntua turvattomammalta.

Vaikka FIDO2-tunnistautumisella on monia etuja salasanatunnistautumiseen verrattuna, täytyy silti ottaa huomioon sen monet käytettävyyteen liittyvät haasteet. Yksi FIDO2:n suurimmista haasteista on tunnistautumislaitteen katoaminen. Koska tunnistautuminen perustuu laitteeseen, sen katoaminen tarkoittaa käytännössä kirjautumiskyvyn menettämistä. Tähän FIDO-liittouma esittää ratkaisuksi useamman FIDO2-tunnisteen käyttöä rinnakkain mahdollisten ongelmatilanteiden välttämiseksi tunnistautumislaitteen kadotessa. [8]

FIDO2-tunnistautuminen on myös yleisesti yhdistetty vain yhteen laitteeseen, mikä aiheuttaa ongelmia, kun käyttäjä haluaa kirjautua johonkin palveluun toisella laitteella, kuin mitä on käytetty palvelussa käytetyn tilin luomisessa. Vaikka tähänkin ongelmaan on ratkaisuja, ne voivat tuntua monelle käyttäjälle huomattavasti haastavammalta, kuin salasanatunnistautuminen. Monet eivät ole tietoisia salasanatunnistautumisen ongelmista. Peruskäyttäjien tietämys FIDO2:sta tai yleisesti salasanattomasta tunnistautumisesta on vähäistä. Puutteellinen ymmärrys salasanaturvallisuudesta, johtaa salasanojen uudelleenkäyttöön ja varomattomaan toimintaan salasanojen kanssa. Sellaiset henkilöt, joilla on puutteellinen ymmärrys salasanaturvallisuudesta hyötyisivät FIDO2:ta todellisuudessa eniten.

3 Ongelmakohtien ratkaiseminen

3.1 Palveluntarjoajien FIDO2 adoptio

FIDO2 saavuttaisi suuremman käyttäjäkunnan mikäli useampi palvelu tarjoaisi ensisijaisena tunnistautumismenetelmänään FIDO2-tunnistautumisen. Tämän lisäksi useat eri teknologiat tukevat heikosti FIDO2-tunnistautumista. Käyttäjät mainitsivat yrityskäyttäjiin kohdistuvassa käyttäjätutkimuksessa puutteiden kohdistuvan mm. VPN (Virtual Private Network), palvelin, sekä tietokoneella kirjautumiseen. Vastaajat huomioivat myös käyttäjäkokemuksen merkittävyyden ja miten käyttökokemuksen täytyy olla samankaltainen eri alustoilla.[9]

Monet olemassa olevat yritysten käyttämät järjestelmät käyttävät salasanoja. Osa näistä on jaettuja salasanoja ja osa henkilökohtaisia. Salasana-arkkitehtuurin korvaaminen salasanattomalla voi tuoda lisäkuluja yrityksille, mutta myös säästöjä erityisesti näiden yritysten palkkaamien asiantuntijoiden ajan säästön sekä vähenevien tietoturvarikkeiden kannalta. Kun Google otti käyttöön FIDO2-tunnistautumisen, kirjautuminen tileille – jotka käyttivät FIDO2-tunnistautumista – nopeutui 40 % verrattuna salasanatunnistautumista käyttäviin tileihin [5]. Tämä nopeutuminen näkyy periaatteessa suoraan työntekijöiden tehokkuudessa, mutta käytännössä pelkkä kirjautumiseen kuluva aika on mitätön suhteessa työpäivän pituuteen. Sen sijaan salasanavaihtojen ja salasanoihin liittyvän tietoturvan ylläpitämiseen kuluvan ajan yhteisvaikutus on jo merkittävä. Kun salasanoja ei ole, ei ole syytä olla yhteydessä

tekniseen tukeen [10]. Kaiken tämän lisäksi kirjautumisiin kuluva aika kertaantuu nopeasti, kun käytössä on useita eri palveluita, jotka tarvitsevat tunnistautumista. Kaiken tämän ajan voisi säästää ottamalla käyttöön FIDO2-tunnistautumisen.

Palvelut, jotka käyttävät FIDO2 tunnistautumista hyötyvät sen kirjautumisen nopeudesta ja turvallisuudesta ja ovat siten houkuttelevia monille yrityksille ja tehokäyttäjille. Peruskäyttäjät eivät kuitenkaan todennäköisesti vaihda salasanattomaan tunnistautumiseen muutoksen subjektiivisen vaivallisuuden vuoksi [10].

3.2 FIDO2 tunnettavuus

Moni ei tiedä FIDO2:ta ellei ole kiinnostunut kyberturvallisuudesta tai vaihtoehtoisista tunnistautumismenetelmistä. FIDO-liittouma voisi tehdä työtä sen eteen, että FIDO2 tunnistautumista tarjottaisiin FIDO-liittouman jäsenten tarjoamissa palveluissa ensisijaisena tunnistautumismenetelmänä. Koska FIDO-liittouman jäseninä toimii suuria yrityksiä, joiden palveluita suuri osa ihmisistä käyttää, johtaisi ensisijaisuus tunnistautumismenetelmänä vähintäänkin FIDO2 tunnettavuuden yleistymiseen ellei jopa suurempaan adoptioon.

FIDO-liittouma voisi myös käyttää sosiaalista mediaa ja mainontaa hyväksi. Tietoiskut salasanaturvallisuudesta ja FIDO2:n tarjoamasta paremmasta vaihtoehdosta nostaisi tietoisuutta salasanattomasta tunnistautumisesta, sekä tukisi sellaisia henkilöitä, jotka eivät halua vaihtaa pois salasanoista tunnistamaan hyviä käytäntöjä salasanojen kannalta.

3.3 Laajempi laitevalikoima ja tuki

FIDO2-standardia tukevien laitteiden valikoima ja niiden laitteiden valmistajien määrä on tällä hetkellä varsin pieni. Osaltaan tämä varmasti johtuu siitä, että kiinnostus FIDO2:ta kohtaan on pientä ja sen myötä kaupallinen saturaation on saa-

vutettu. Toisaalta kiinnostus FIDO2:ta kohtaan voisi kasvaa, mikäli olisi laajempi tuotevalikoima. Monet tuotteet mainostavat erilaisia teknologioita, joita ne käyttävät. Tuotteiden myyntisivulla tai tuotepakkauksessa on usein merkintöjä ja logoja teknologioista, joita ne tukevat. FIDO2 ja sitä tukevat laitteet voisivat hyötyä samanlaisesta mainonnasta.

Myös olemassa olevat tuotteet voivat tukea FIDO2:ta. Jotkin tietokoneet sisältävät FIDO2:n tarvitseman TPM:n. Olemassa olevien tuotteiden kategoriasta on kuitenkin vaikeampi tunnistaa FIDO2:ta tukevat laitteet. Peruskäyttäjä ei välttämättä tiedä, että TPM:n sisältävä tietokone tukee FIDO2:ta, joten pelkkä maininta TPM:stä ei aina riitä. FIDO-liittouma voisi tehdä sivun, jolla käyttäjä voisi tarkistaa tukeeko hänen tuotteensa FIDO2:ta.

3.4 Luottamuksen kasvattaminen

FIDO2:n tietoturvan kehittäminen on olennaista luottamuksen kasvattamiseksi. Aiemmin FIDO2:ta koskenut tietoturvaongelma ei nostanut luottamusta siihen, muttei todennäköisesti ole enää merkittävä tekijä sen adoptiossa. FIDO2:n turvatakuut ovat pohjustettu olettamuksella, ettei alustalla ole haittaohjelmia. Samat turvatakuut eivät pidä paikkaansa haittaohjelmien ollessa alustalla.[11]

FIDO-liittouman pitää tehdä jatkuvaa PR-työtä luottamuksen kasvattamiseksi ohittaakseen salasanapohjaisen tunnistautumisen johtavana tunnistautumismenetelmänä. Yksi vaihtoehdoista olisi jatkuvien turvallisuuspäivitysten julkaisu, testaus ja aiemmista versioista tehtyjen löytöjen julkaisu. FIDO-liittouman tulisi kuitenkin käyttää kolmansien osapuolien palveluita tähän tutkimustyöhön puolueellisuuden välttämiseksi. Toinen asia, mistä FIDO-liittouma voisi hyötyä, on käyttäjäkyselyiden tekeminen. Näiden kyselyiden avulla FIDO-liittouma voisi saada tietoa suurimmista syistä, miksi FIDO2:ta ei haluta käyttää tai miksi siihen ei luoteta. Tämän myötä olisi helpompaa tehdä merkittäviä muutoksia, joko siihen miten FIDO2 toimii

käytännössä tai tiedotukseen FIDO2:n toiminnasta ja merkityksestä kyberturvallisuudessa.

I. Loutfin tekemässä analyysissä hän arvioi, että käyttäjän on luotettava FIDO-liittoumaan, palvelun tarjoajaan, laitteiden valmistajiin, tietokonealustaan, käyttäjään eli toisinsanoen itseensä ja FIDO:n protokolliin. Käyttäjän on siis luotettava, että FIDO-liittouma on tunnistanut oikeat kokoelmat metadataa tunnistaakseen luotettavat osapuolet, että FIDO-liittouma sertifioi ainoastaan luotettavia palveluita ja että FIDO:n julkisen avaimen infrastruktuuri on turvallinen ja validi. Käyttäjän on myös luotettava, ettei tietokonealustassa ole haittaohjelmia, ettei käyttäjä itse ole altistanut sitä haittaohjelmille ja, että käyttäjän käyttämät tunnistautumislaitteet ovat turvallisia. [12]

3.5 Käytettävyyden korjaaminen

Käytettävyyden korjaamisessa voidaan käytännönopetusta FIDO2-tunnistautumisessa. Yksi käyttäjien suurimmista haasteista on puutteellinen kokemus ja tietämys. Erityisen hankaliksi käyttäjät kokevat FIDO2:n käyttöönoton eri palveluissa sekä rajatapaukset, kuten kadonneen tunnistautumislaiteen käsittelyn. [9] [10]

Eräs ratkaisu tilinperustamiseen liittyviin haasteisiin on Passkey-synkronointi. Tässä tapauksessa Passkey-tunnus – joka luodaan yhdellä laitteella – synkronoidaan käyttäjän muille laitteille, jotka käyttävät samaa käyttöjärjestelmää ja ovat kirjautuneena samalle alustatilille. Alustatilillä tarkoitetaan käyttäjätiliä, jolla voidaan kirjautua usealle eri käyttäjän laitteelle, kuten Microsoft tili. Tämä kuitenkin luo ongelmia tietoturvan kannalta, sillä synkronointiin käytetään salasanaa, joka on altis kalastelulle ja yksityisavain voi vuotaa synkronoidessa. Francisco ehdottaa tilin perustamiseen parannuksia, jotka korjaavat monia käyttäjien haasteita sekä tietoturvaongelmia. Yksi ehdotuksista on salasanaton Passkey-synkronointi.[8] Salasanattomaan Passkey-synkronointiin ei syvennytä tässä kirjallisuuskatsauksessa.

4 FIDO2 käyttöönoton tulevaisuus

4.1 Yksityisten henkilöiden FIDO2 käyttö

Yksityishenkilöt kokivat suurimmaksi haasteeksi käytettävyyden. Lyastani ja muut tutkivat käyttäjätutkimuksissa yksityishenkilöiden sekä yritysten työntekijöiden kokemaa FIDO2:n käytettävyyttä ja käyttökelpoisuutta kaksivaiheisen ja yksivaiheisen tunnistautumisen kanssa. Tutkimus pyrkii myös vastaamaan, ovatko käyttäjät valmiita vaihtamaan tietopohjaisesta tunnistautumisesta omistuspohjaiseen tunnistautumiseen. [13]

Käyttäjätutkimuksen mukaan peruskäyttäjät ovat tyytyväisiä salasanattomaan tunnistautumiseen ja valmiita hyväksymään sen, vaikka heillä onkin huolia tilanteesta, jossa tunnistautumislaite katoaa ja tili – johon tunniste on liitetty – menetetään. Käyttäjät kokevat myös ongelmalliseksi FIDO2:n joustamattomuuden julkisia tietokoneita – joilla ei ole tarvittavia liitäntöjä tunnistautumislaitetta varten – käytettäessä ja tilanteissa, joissa käyttäjä haluaa jakaa tilin luotetun henkilön kanssa. [13]

Käyttäjät kokevat erilliset laitteet hankaliksi ja käytännöllisyys on merkittävämpi tekijä uuden tunnistautumismenetelmän adoptiossa, kuin turvallisuus [13]. Tämän puolesta olemassa olevat tunnistusta tukevat laitteet, kuten älypuhelimet tulevat todennäköisesti olemaan suositumpia FIDO2-tunnistautumisvälineenä, kuin ulkoiset tunnistautumislaitteet. Käyttäjät välttävät kaksivaiheista tunnistautumista

epäkäytännöllisyyden vuoksi [13].

Lyastani ja muut viittaavat Das:in ja muiden tekemään käyttäjätutkimukseen, jossa todettiin, että tunnistautumislaitteiden suunnittelussa ei oltu huomioitu vanhempien ikäluokkien tarpeita, ja sen myötä turva-avaimien ja ulkoisten tunnistimien adoptio on vähäisempää vanhemmilla ikäluokilla. [13] On epätodennäköistä, että vanhempien ihmisten turva-avain adoptio nousee ilman, että suunnitellaan heille kohdennettuja turva-avaimia.

Lyastanin ja muiden käyttäjätutkimuksen kvantitatiivisten mittausten perusteella FIDO2-tunnistautuminen on käytettävämpi, kuin salasanatunnistautuminen. Turvallisuus ei ollut tilastollisesti merkittävä tekijä käytettävyyden mittaamisessa. Kvalitatiivisten mittausten perusteella FIDO2-tunnistautuminen vähensi kognitiivista ja muistamisen kuormaa, mikä koettiin suureksi eduksi. Pelot tilin menettämisen syystä muuttuivat heikoista salasanoista ja kalastelusta tunnistautumislaitteen ja tilin menettämiseksi tai vääriin käsiin päätymiseksi. Epäyhteensopivuudet ulkoisten tunnistautumislaitteiden ja mobiililaitteiden välillä koettiin epäkäytännöllisiksi. [13] Testissä ei kuitenkaan oteta huomioon mahdollisuutta käyttää mobiililaitetta tunnistautumisvälineenä. Samaan tiliin voi liittää turva-avaimen ja mobiililaitteen tunnistautumisvälineeksi.

Mentaalisten mallien merkitys adoptiossa on otettu huomioon. Monilla on positiivisia kokemuksia salasanojen käytöstä. Käyttäjät ymmärtävät miten salasanat toimivat, mutta vastaavaa kokemusta FIDO2:ta ei vielä ole, joten käyttäjä voi kokea salasanattoman vaihtoehdon haastavaksi. Käyttöön liittyvää kokemattomuutta koettiin niin turva-avaimen kuin sisäisen varmentimen käytössä. Käyttäjä ei aina osannut laittaa turva-avainta oikeaan porttiin tai tiennyt miten tunnistautumislaitetta käytetään. [13] Kokemukseen liittyvät huolet, ennakkoluulot ja osaamattomuus todennäköisesti ratkeaa ajan myötä.

4.2 Yritysten FIDO2 käyttö

Kepkowski ja muut käyttivät hyväksi toimialan kirjallisuuskatsauksia ja käyttäjätutkimuksia saadakseen koko kuvan FIDO2:n haasteista yritystoiminnassa. Yhteensä he käyttivät neljää eri kirjallisuuskatsausta lähteenä, joista saatiin riittävän edustava näyttö FIDO2:n yrityskäyttötapauksista.[9]

Identiteetin- ja pääsynhallinnalta vaaditaan eri asioita eri kokoisissa yrityksissä. Tämän myötä tunnistautumismenetelmät tarvitsevat joustavuutta – ei pelkästään yritysten sisäisten vaatimuserojen vuoksi vaan myös – yritysten välisten vaatimuserojen vuoksi. Mikäli jokin yritys ottaisi käyttöön FIDO2:n pääasiallisena tunnistautumismenetelmänä, sen tulisi harkita tarkkaan, mitä erilaisia tunnistautumismenetelmiä tai laitteita se sallii FIDO2-tunnistautumisessa. [9] Yritysten täytyisi myös tehdä joko sisäistä kehitystä yrityksen infrastruktuurissa FIDO2:n käyttöönotossa tai nojata muiden palveluntarjoajien tarjoamiin vaihtoehtoihin, jotka ovat vielä rajattuja.

Salasanapohjaisen tunnistautumisen taustaprosessit, kuten salasanojen palauttaminen ja tilien deaktivointi osataan yleisesti ottaen hyvin. FIDO2:n kohdalla näihin taustaprosesseihin tulee kuitenkin muutoksia, jotka monimutkaistavat ja vaikeuttavat niitä niin ylläpitäjän, kuin käyttäjänkin näkökulmasta [9]. Yritysinfrastruktuurin muutokset siirtyessä salasanatunnistautumisesta salasanattomaan tunnistaumiseen ovat perustavanlaatuisia, kalliita ja työläitä, mutta ne voivat olla vaivan arvoisia, kun otetaan huomioon tietoturva edut sekä yrityksen työntekijöiden tunnistautumisessa kumulatiivisesti säästynyt aika.

Ulkoisen varmentimen saattaminen tunnistautuvalle henkilölle on haasteellista, koska varmennin voidaan kloonata, sitä voidaan muokata tai avain tunnistimen sisällä voidaan varastaa. Nämä ongelmat voidaan ratkaista kuitenkin erinäisten fyysisten ja ohjelmistollisten menetelmien avulla. Muokattu varmennin voidaan tunnistaa tiivistefunktion avulla. Varmentimen kloonaaminen voidaan estää lataamalla laiteoh-

jelmisto viiveellä, niin ettei sitä voida kopioida. Varmentimen sisältämät avaimet voidaan salata kryptografistesi. Itse varmennin voidaan paketoida, niin ettei sitä voida muokata tai käyttää, ilman että siitä jää jälkiä paketointiin. [9]

Varmentimen yhdistäminen johonkin henkilöön tai identiteettiin turvallisesti on seuraava haaste. Se voidaan kuitenkin tehdä varmentimen antamisen yhteydessä, jolloin varmentimen saajan identiteetti voidaan tarkistaa. Varmennin voidaan myös yhdistää täysin uuteen tiliin tai käyttää valmiiksi olemassa olevaa tietoa tilin, käyttäjän ja varmentimen yhdistämiseksi. Valmiiksi olemassa olevaan tiliin voidaan myös yhdistää varmennin. [9]

Googlen tekemässä kokeilussa – jossa työntekijöille jaettiin 50000 turva-avainta – todettiin, että turva-avain on helppo ottaa käyttöön ja sitä on helpompi käyttää, kuin kertakäyttöisiä salasanoja käyttävä kaksivaiheinen tunnistautuminen. [13]

Ajan myötä yritykset vaihtavat laitteistoa säästääkseen ylläpitokustannuksista. FIDO2-tunnistautumiseen käytetyt alustapohjaiset varmentimet tai ulkoiset varmentimet eivät ole poikkeuksellisia tämän suhteen. Tyypillisesti varmentimilta haluttu turvallisuusominaisuus, joka estää tunnistautumiseen käytettävien yksityisten avainten ulos viemisen, aiheuttaa käytettävyyshaittaa. Koska avaimia ei saa siirrettyä uudelle laitteelle, ainoa vaihtoehto on rekisteröidä ja yhdistää uusi laite aikaisemmalle tilille joka kerta, kun laitevaihdos tehdään. Vanhat ulkoiset varmentimet voivat myös olla yhteensopimattomia uudempien laitteiden kanssa. [9] Laitteiden uusiminen, uusien laitteiden rekisteröiminen ja yhdistäminen on merkittävästi ihmisresurssi-intensiivisempää, kuin salasanan vaihtaminen. Teknologian kehittyessä tämä voi kuitenkin helpottua, mutta siihen asti on todennäköisempää, että FIDO2:ta käytetään ainoastaan korkeaa tietoturvallisuutta vaativissa tehtävissä.

Kun jonkin käyttäjän tai työntekijän tili tarvitsee lakkauttaa, se on yhtä helppoa, kuin salasanatunnistautumiseen perustuvissa ratkaisuissa. Tunnistautumispalvelimelta täytyy vain poistaa kyseiseen tiliin liittyvä julkinen avain. Sen sijaan käyttä-

jän näkökulmasta tilanne on haastavampi, kuin salasanatunnistautumisessa. Avain, jota käytetään tunnistautumiseen, täytyy poistaa laitteelta avaintallennustilan ollessa rajallista. [9] Tyypillisesti salasanapohjainen tunnistautuminen ei vaadi käyttäjän puolesta mitään toimia tilin lakkauttamisessa.

FIDO2-tunnistautumisen tuki erilaisilla laitteilla on rajallista. Kannettavien tietokoneiden ja pöytätietokoneiden tuki FIDO2:lle erityisen puutteellista. Yleisesti etätyöhön tarvittavat sovellukset, kuten VPN:t, eivät kaikki tue FIDO2-tunnistautumista, mikä vaikeuttaa FIDO2:n käyttöönottoa. Yritysinfrastruktuuri ja useat työkalut eivät myöskään tue FIDO2:ta, mikä käytännössä estää täysin tiettyjä työtekijöitä käyttämästä FIDO2:ta näissä tilanteissa. [9] Päädytään siis tilanteeseen, missä käytetään salasanatonta tunnistautumista ja salasanatunnistautumista rinnakkain, eikä saada täyttä hyötyä salasanattomasta tunnistautumisesta.

Jotkin yritysten käyttämät ohjelmistot tukevat vain yhtä paikallista tiliä. Jos tälle tilille tunnistaudutaan FIDO2:n avulla, täytyy tämä tunnistautumismenetelmä jakaa kaikkien niiden kesken, jotka tarvitsevat pääsyn kyseiseen ohjelmaan. FIDO2 ei itsessään tue valtuuksien jakamista, toisin sanoen yksi valtuus on liitettynä yhteen tiliin. [9] Tämä aiheuttaa erityisesti ongelmia etätyötilanteissa, joissa tunnistautumiseen käytetty varmennin ei ole kaikkien saatavilla.

Yritysmaailmassa käytetyt FIDO2-varmentimet ovat yhtä alttiita katoamiselle kuin muutkin. FIDO2:n tekniset ominaisuudet tekevät tilin palauttamisesta varmentimen kadotessa haastavaa, ellei käyttäjä ole luonut tarvittavia palautusmenetelmiä. Palauttamiseen voidaan käyttää yrityksen teknistä tukea, toista varmennin-ta, joka on liitetty samaan tiliin tai kertakäyttöistä salasanaa. Tekninen tuki pystyy auttamaan työntekijää rajatun käyttäjämäärän vuoksi, mutta on altis sosiaaliselle manipuloinnille. Kertakäyttöisellä salasanalla on samat ongelmat kuin muillakin salasanoilla, eli arvattavuus ja vuotamisriski. [9]

5 Yhteenveto

Tutkielman päätutkimuskysymyksenä esitettiin "mitkä asiat vaikuttavat FIDO2:n käytön helppouteen tai vaikeuteen"ja sen rinnalla esitettiin tukevina tutkimuskysymyksinä "voiko FIDO2 korvata salasanat"ja "miltä näyttää FIDO2:n tulevaisuus."

Kirjallisuuskatsauksessa päätutkimuskysymystä tutkittiin yksityishenkilön ja yrityksen näkökulmasta. Lopputuloksena todettiin, että käytettävyyttä vaikeuttaa FIDO2:n rakenteelliset ominaisuudet, kuten sen käyttöönoton ja tilinpalauttamisen vaikeus, useiden tunnistimien rinnakkaisen käytön tuomat ongelmat sekä puutteellinen tuki palveluntarjoajilta. Helpottavina ominaisuuksina koettiin salasanattomuus ja sen myötä muistamiseen liittyvien ongelmien poistuminen ja tunnistautumisen nopeus.

FIDO2 kelpaa salasanojen korvaajaksi tietoturvan näkökulmasta, mutta käyttöönoton ongelmien perusteella se ei tule korvaamaan salasanoja vielä vähään aikaan. Tietoturva ongelmat eivät kuitenkaan katoa, vaan ne muuttuvat. Salasanojen suurimmat ongelmat kalastelu ja vuotaminen vain vaihtuvat FIDO2:n suhteen haittaohjelmista seuraavaan suurempaan uhkaan. Käyttäjätutkimuksissa huomattiin, että käytettävyys on jo monien mielestä riittävän hyvä salasanatunnistautumisesta FIDO2-tunnistautumiseen vaihtamiseen. Käyttäjien mielestä turvallisuus on kuitenkin toissijaista käytettävyyden rinnalla, jonka kanssa FIDO2:lla on edelleen haasteita. Käyttöönotto koetaan erityisen haastavaksi, kun taas itse käyttäminen koetaan jopa helpommaksi kuin salasanapohjaisen tunnistautumisen käyttäminen.

Erityisesti yritysten näkökulmasta FIDO2:n tulevaisuus näyttää vielä heikolta, koska työkalut ja infrastruktuuri tukevat FIDO2:ta heikosti. Laajempi käyttöönotto on kuitenkin vasta alkuvaiheilla, eli tilanne voi vain mennä parempaan suuntaan. Yksityiskäyttäjien näkökulmasta tilanne on kuitenkin jo parempi, koska laajempi käyttöönotto on pidemmällä. Useat suurempien yritysten yksityishenkilöille tarjoamat palvelut hyväksyvät FIDO2:n ensisijaisena tunnistautumismenetelmänä, mutta vielä on pitkä matka todelliseen salasanattomuuteen.

Lähdeluettelo

[1] *FIDO Alliance*, FIDO. url: https://fidoalliance.org/fido2/ (viitattu 13. 05. 2024).

[2] Verizon, *Data Breach Investigations Report*, 2020. url: https://www.verizon.com/business/en-gb/resources/reports/2020-data-breach-investigations-report.pdf (viitattu 13. 05. 2024).

[3] *Guide to Web Authentication*, Guide to Web Authentication. url: https://webauthn.guide/ (viitattu 29. 02. 2024).

[4] *How FIDO Works - Standard Public Key Cryptography User Privacy*, FIDO Alliance. url: https://fidoalliance.org/how-fido-works/ (viitattu 13. 05. 2024).

[5] *Passwordless by default: Make the switch to Passkeys*, Google. url: https://blog.google/technology/safety-security/passkeys-default-google-accounts/ (viitattu 13. 05. 2024).

[6] G. Cooper, B. Behm, A. Chakrabotry et al., toim., *FIDO Device Onboard Specification 1.1*. url: https://fidoalliance.org/specs/FDO/FIDO-Device-Onboard-PS-v1.1-20220419/FIDO-Device-Onboard-PS-v1.1-20220419.pdf (viitattu 11. 04. 2024).

[7] M. Barbosa, A. Boldyreva, S. Chen ja B. Warinschi, *Provable Security Analysis of FIDO2*, Cryptology ePrint Archive, Paper 2020/756, https://eprint.

iacr.org/2020/756, 2020. url: https://eprint.iacr.org/2020/756 (viitattu 13. 05. 2024).

[8] F. Corella, "Overcoming the UX Challenges Faced by FIDO Credentials in the Consumer Space", teoksessa *HCI for Cybersecurity, Privacy and Trust*, A. Moallem, toim., Cham: Springer Nature Switzerland, 2023, s. 447–466, ISBN: 978-3-031-35822-7.

[9] M. Kepkowski, M. Machulak, I. Wood ja D. Kaafar, "Challenges with Passwordless FIDO2 in an Enterprise Setting: A Usability Study", teoksessa *2023 IEEE Secure Development Conference (SecDev)*, 2023, s. 37–48. DOI: 10.1109/SecDev56634.2023.00017.

[10] K. Bicakci ja Y. Uzunay, "Is FIDO2 Passwordless Authentication a Hype or for Real?: A Position Paper", teoksessa *2022 15th International Conference on Information Security and Cryptography (ISCTURKEY)*, 2022, s. 68–73. DOI: 10.1109/ISCTURKEY56345.2022.9931832.

[11] D. Kuchhal, M. Saad, A. Oest ja F. Li, "Evaluating the Security Posture of Real-World FIDO2 Deployments", teoksessa *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, sarja CCS '23, Copenhagen, Denmark: Association for Computing Machinery, 2023, s. 2381–2395, ISBN: 9798400700507. DOI: 10.1145/3576915.3623063. url: https://doi.org/10.1145/3576915.3623063.

[12] I. Loutfi ja A. Jøsang, "FIDO Trust Requirements", teoksessa *Secure IT Systems*, S. Buchegger ja M. Dam, toim., Cham: Springer International Publishing, 2015, s. 139–155, ISBN: 978-3-319-26502-5.

[13] S. Ghorbani Lyastani, M. Schilling, M. Neumayr, M. Backes ja S. Bugiel, "Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication", teoksessa *2020 IEEE Symposium on*

Security and Privacy (SP), 2020, s. 268–285. DOI: 10.1109/SP40000.2020.00047.