jamk

Monivaiheinen todentaminen Cisco Duo -tuotteella

Miro Hiljanen

Opinnäytetyö, AMK
Maaliskuu 2024
Tietojenkäsittely ja tietoliikenne
Insinööri (AMK), tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Hiljanen, Miro

Monivaiheinen todentaminen Cisco Duo -tuotteella

Jyväskylä: Jyväskylän ammattikorkeakoulu. Maaliskuu 2024, 104 sivua.

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Laajasti ympäri Suomea toimiva Frendy Oy tunnisti tarpeen vahvistaa organisaationsa tietoturvaa erityisesti keskittymällä tunnistautumismenetelmien parantamiseen. Projektin päämääränä tarjota pienille ja keskisuurille yrityksille turvallisuusratkaisu, joka ei vaadi Microsoft Entra ID:tä, mutta on yhteensopiva sen kanssa tulevaisuudessa. Valitsimme Cisco Duon monivaiheisen todentamisen tämän tavoitteen saavuttamiseksi varmistaen, että se voidaan integroida saumattomasti Microsoft Entra ID:n kanssa, kun yritykset ovat valmiita tai tarvitsevat sitä. Tämä lähestymistapa takaa joustavuuden ja skaalautuvuuden yritysten turvallisuustarpeisiin. Tavoitteena oli lisätä käyttäjätunnuksen ja salasanan yhdistelmän turvallisuutta tarjoamalla helppokäyttöinen ratkaisu loppukäyttäjille. Lisäksi tavoitteena oli syventyä ja tutustua digitaaliseen ja monivaiheiseen todentamiseen yleisesti sekä vertailla eri monivaiheisen todentamisen palveluntarjoajia keskenään.

Toteutustavaksi valikoitui yhteistyössä suunniteltu pilottiprojekti, jossa Cisco Duon monivaiheisen todentamisen ratkaisua testattiin yrityksen IT-infrastruktuurissa. Projektiin sisältyi tekninen suunnittelu, ratkaisun konfigurointi ja testikäyttäjän kautta tapahtuva käytännön testaus. Toteutuksen aikana painotettiin erityisesti käyttäjäkokemuksen sujuvuutta ja turvallisuuden parantamista.

Tuloksena havaittiin, että Cisco Duon käyttöönotto paransi merkittävästi tietoturvaa monivaiheisessa todentamisessa vähentäen onnistuneesti haavoittuvuuksia todentamisprosessissa käyttäen niissä monipuolisesti eri menetelmiä. Lisäksi käyttäjäkokemus todettiin samalla positiiviseksi käyttäjien raportoidessa todentamisprosessin olevan sekä nopeampi että käyttäjäystävällisempi toiminnallisuudeltaan.

Johtopäätöksenä projektista todettiin, että yleisesti monivaiheisen todentamisen käyttöönotto on tärkeä askel kohti vahvempaa tietoturvaa. Suositellaan jatkuvaa kehitystä ja uusien teknologioiden hyödyntämistä tietoturvan parantamiseksi ottaen huomioon käyttäjien tarpeet ja käyttökokemus. Projektin perusteella Frendy Oy suunnittelee jatkavansa Cisco Duon käyttöä ja laajentavansa sen käyttöönottoa koko organisaatiossa sekä myöhemmin asiakkailleen.

Avainsanat (asiasanat)

Monivaiheinen todentaminen, Käyttöönotto, Tietoturva, Todentamisprosessi, Digitaalinen identiteetti, Microsoft Azure Active Directory, Microsoft Entra ID, PK-yritykset, Cisco Duo, Frendy, Toimintatutkimus

Muut tiedot (salassa pidettävät liitteet)

Esim. opinnäytetyön liitteen salassapitoperuste, ks. raportointiohjeen luku 4.1.2

jamk

Description

Hiljanen, Miro

Multi-Factor Authentication with Cisco Duo product

Jyväskylä: JAMK University of Applied Sciences, March 2024, 104 pages.

Information and Communications. Degree Programme in Information and Communication Technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

Frendy Oy, operating extensively throughout Finland, recognized the need to enhance its organizational cybersecurity, especially by focusing on improving authentication methods. The project's goal was to offer small and medium-sized enterprises a security solution that does not require Microsoft Entra ID but is compatible with it for future integration. We selected Cisco Duo's multi-factor authentication to achieve this goal ensuring it could be seamlessly integrated with Microsoft Entra ID when businesses are ready or need it. This approach ensures flexibility and scalability for businesses' security needs. The aim was to enhance the security of the username and password combination by providing an easy-to-use solution for end-users. Moreover, the objective was to delve into and familiarize ourselves with digital and multi-factor authentication in general, as well as to compare different multi-factor authentication service providers.

The implementation method chosen was a collaboratively designed pilot project, in which Cisco Duo's multi-factor authentication solution was tested in the company's IT infrastructure. The project included technical design, solution configuration, and practical testing through a test user. During the implementation, special emphasis was placed on the smoothness of the user experience and enhancing security.

As a result, it was observed that the deployment of Cisco Duo significantly improved cybersecurity in multi-factor authentication, successfully reducing vulnerabilities in the authentication process by employing a variety of methods. Additionally, the user experience was found to be positive, with users reporting that the authentication process was both faster and more user-friendly in functionality.

In conclusion, the project found that the adoption of multi-factor authentication is an important step toward stronger cybersecurity. Continuous development and the use of new technologies to improve cybersecurity are recommended, taking into account user needs and experience. Based on the project, Frendy Oy plans to continue using Cisco Duo and to expand its deployment across the entire organization and later to its customers.

Keywords/tags (subjects)

Multi-factor authentication, Implementation, Cybersecurity, Authentication process,Digital identity Microsoft Azure Active Directory, Microsoft Entra ID, SMEs (Small and Medium-sized Enterprises), Cisco Duo, Frendy, Action research

Miscellaneous (Confidential information)

For example, the confidentiality marking of the thesis appendix, see Project Reporting Instructions, section 4.1.2

Sisältö

Kuviot

Taulukot

Lyhenteet

2FA	Two-Factor Authentication
AAD	Microsoft Azure Active Directory
AAL2	Authenticator Assurance Level 2
AD	Microsoft Active Directory
AD DS	Microsoft Active Directory Domain Services
AI	Artificial intelligence
AiTM	Adversary in the Middle Attack
ARP	Address Resolution Protocol
B2B	Business-to-business
CA	Conditional Access
CISA	Certified Information Systems Auditor
CSP	Content Security Policy
DNS	Domain Name System
FIDO	Fast Identity Online
IAM	Identity and Access Management
LLMNR	Link-Local Multicast Name Resolution
MFA	Multi-Factor Authentication
NFC	Near-field communication
NIST	National Institute of Standards and Technology
OATH	Hardware token, Software token
OOBE	Out-of-box experience
OTP	One Time Password
OU	Organizational unit
RP	Relying party
SaaS	Software as a Service
SS7	Signaling System 7
SSL	Secure Sockets Layer
SSS	Security and Safety Service
TLS	Transport Layer Security
TOTP	Time-based one-time password

TPM	Trusted Platform Module -turvapiiri
U2F	Universal 2nd Factor
VoIP	Voice over IP
VPN	Virtual private network
W3C	World Wide Web Consortium

1 Johdanto ja lähtökohdat

Toimeksiantajana opinnäytetyössä toimi Frendy Oy. Frendy Oy, mikä on ympäri Suomen toimiva IT-palveluyritys, joka sai alkunsa vuonna 2021. Frendyn palveluksessa on kokonaisuudessaan noin 360 työntekijää ja yritys koostuu sekä miehistä että naisista. Yrityksen perusajatuksena on tarjota ratkaisuja pienille ja keskisuurille yrityksille sekä auttaa pienellä kynnyksellä korkeaa teknistä osaamista vaativissa ongelmatilanteissa, jotta yritykset eivät itse joudu olemaan IT-asiantuntijoita vaan he voivat keskittyä työntekoon. Frendyn päätehtävänä on taata asiakkaidensa liiketoiminnan laatu ja sujuvuus, ja sen tavoitteen he lupaavat saavuttaa yhdistämällä vahvaa liiketalouden osaamista ja syvää teknistä asiantuntemusta. Frendy on sitoutunut tukemaan asiakkaitaan IT-haasteissaan, jotta he voivat nimenomaan keskittyä ydintoimintaansa huoletta ja luottavaisin mielin. (Yritys n.d.)

Korpin (2023) mukaan tässä opinnäytetyössä yhtenä isona lähtökohtana ja tavoitteena oli Frendylla halu tutkia Cisco Duon monivaiheisen todentamisen sopivuus heidän asiakkailleen lähinnä PK-yritysten osalta, joilla ei ollut ollenkaan Microsoft Entra ID:tä käytössä ympäristössään tai siellä ei ollut Microsoft Entran monivaiheisen todentamisen käyttöön riittäviä lisenssejä (Korppi 2023). Karhula (2023) avaa lisäksi, että Cisco Duo integroituu muihin Frendy Oy:n käyttämiin Ciscon palveluihin hyvin ja tätä vahvistaa lisäksi syvällä olemassa oleva kumppanuus Ciscon kanssa (Karhula 2023). Opinnäytetyön päämääränä oli tarjota pienille ja keskisuurille yrityksille turvallisuusratkaisu, joka ei vaadi Microsoft Entra ID:tä, mutta on yhteensopiva sen kanssa tulevaisuudessa. Valitsimme Cisco Duon monivaiheisen todentamisen tämän tavoitteen saavuttamiseksi varmistaen, että se voidaan integroida saumattomasti Microsoft Entra ID:n kanssa, kun yritykset ovat valmiita tai tarvitsevat sitä. Tämä lähestymistapa takaa joustavuuden ja skaalautuvuuden yritysten turvallisuustarpeisiin. Käyttöönottamisella pyritään kehittämään jatkossa Frendyn asiakasyritysten tietoturvaa hyödyntäen Cisco Duon monivaiheista todentamista käyttäjien kirjautumisissa. Frendylta työn tilaajana toimi sen tietoturva-puoli, joka halusi ensin testata ja dokumentoida järjestelmän heidän testiympäristössä ennen kuin se siirrettäisiin tuotantoon ja asiakasyrityksille. Työssä kiinnitettiin erityistä huomiota siihen, kuinka kirjautuminen saatiin toimimaan eri vaiheiden jälkeen ja millä perustein se otettiin käyttöön käyttäjille. Tämä opinnäytetyö tukee vahvasti Frendyn tietoturvallisia tavoitteita ja hallintastandardeja, mitkä he haluavat täyttää tulevaisuudessa.

Nykypäivänä tietoturvallisuus ja erilaiset tietomurrot ovat keskeisiä ja ajankohtaisia aiheita, jotka vaikuttavat laajasti yksilöihin ja yrityksiin kuten Frendy, sekä yhteiskuntaan kokonaisuutena. Tietoturvallisuus viittaa toimenpiteisiin ja käytäntöihin, joilla pyritään suojaamaan tietoja, järjestelmiä ja verkkoja, kun taas tietomurrot ovat epäluotettavien tahojen yrityksiä tunkeutua, varastaa tai vahingoittaa tietojärjestelmiä. Nykypäivänä teknologian nopea kehittyminen ja yhä monimutkaisemmat verkkoympäristöt ovat tuoneet mukanaan uusia uhkia ja haasteita tietoturvallisuudelle. Frendy haluaa suorittaa tämän Cisco Duon monikerroksisen tietoturvaratkaisun monivaiheisen todentamisen käyttöönoton, mikä keskittyy erityisesti käyttäjän tunnistukseen ja pääsynhallintaan. Cisco Duo tarjoaa monipuolisia työkaluja organisaatioille varmistaakseen, että vain oikeilla käyttäjillä on pääsy tietoverkkoihin ja -järjestelmiin. Dokumentaation suuri määrä ja selkeys sekä alustan erinomainen käyttöliittymä erottavat sen kilpailijoista. Lisäksi Frendyn tietoturva-puolella on jo ennestään ollut todella hyviä kokemuksia sekä tietoa alustasta ja sen toiminnoista, mitkä tukivat myös tätä Cisco Duon monivaiheisen todentamisen käyttöönottoa.

Tietoturvan alueella monivaiheinen todentaminen on noussut keskeiseksi käsitteeksi, kun pyritään tehostamaan pääsynvalvontaa ja tietojen suojelua. MFA viittaa turvallisuusmenetelmään, jossa käyttäjän on todennettava identiteettinsä useammalla kuin yhdellä todentamisvaiheella ennen kuin hän saa pääsyn tietojärjestelmiin tai -resursseihin. Nämä vaiheet voivat sisältää jotakin seuraavista: jotain, mitä käyttäjä tietää, jotain, mitä käyttäjä omistaa, tai jotain, mikä on käyttäjälle ominaista. Monivaiheisen todentamisen käyttöönotto lisää merkittävästi tietoturvan tasoa, sillä se vähentää huomattavasti riskiä, että tietojärjestelmiin pääsee luvattomasti, vaikka yksi todentamistaso murretaankin. Tämän vuoksi MFA onkin laajalti tunnustettu yhdeksi tehokkaimmista keinoista parantaa tietoturvaa digitaalisessa ympäristössä.

2 Digitaalisen todentamisen teknologia

Todentaminen on keskeinen elementti nykyaikaisten organisaatioiden tietojärjestelmissä ja verkkopalveluissa toimien välttämättömänä prosessina käyttäjien tai laitteiden henkilöllisyyden ja tiettyjen järjestelmien, sovelluksien tai resurssien käyttöoikeuksien varmistamiseksi. Tämä prosessi on tietoturvan olennainen osa, joka estää luvattoman pääsyn ja suojaa tietoja käsittäen laajan kirjon menetelmiä ja teknologioita henkilöllisyyksien varmistamiseksi. Digitaalisen maailman eksponentiaalinen kasvu viime vuosikymmeninä erityisesti sosiaalisen median alustojen, pankkipalveluiden,

verkkokauppojen ja muiden verkkopalveluiden käytön myötä, on tuonut mukanaan monimutkaisuutta ja haasteita. Tämä kasvu herättää kysymyksen: Miten voidaan varmistaa, että käyttäjät ovat todella sitä, keitä he väittävät olevansa. Tämä kysymys on digitaalisen identiteetin ja todentamisen keskiössä. Tehokkaan todentamisjärjestelmän puuttuessa yksilöiden ja yritysten tärkeät tiedot voivat olla alttiina identiteettivarkauksille, petoksille ja tietoturvaloukkauksille.

Grassi, Garcia & Fenton (2020, luku 2) esittelevät, että ihmisen erillinen online-persoona tapahtuman aikana on digitaalinen identiteetti. Vaikka digitaalisen identiteetin ei aina tarvitse yksilöidä kohdetta joka tilanteessa, se on aina ainutlaatuinen digitaalisen palvelun kontekstissa. Toisin sanottuna pelkkä digitaalisen palvelun käyttö ei aina tarkoita, että kohteen todellinen henkilöllisyys on tiedossa. Henkilöllisyyden todentaminen vahvistaa, että henkilö on se, joka hän sanoo olevansa. Prosessi, jolla varmistetaan yhden tai useamman digitaalisen identiteetin vahvistamiseen käytetyn autentikaattorin laillisuus tunnetaan digitaalisena todentamisena. Todentamisen avulla digitaaliseen palveluun pääsyä yrittävä voi todistaa olevansa vastuussa todentamiseen käytetyistä teknologioista. Kun todentaminen onnistuu, on olemassa hyväksyttävät riskiperusteiset takuut siitä, että palvelua nyt käyttää sama henkilö, joka käytti sitä aiemmin. Digitaaliseen todentamiseen liittyvä teknologinen ongelma johtuu siitä, että tämä menettely edellyttää yleensä yksittäisten koehenkilöiden todentamista avoimen verkon kautta päästäkseen digitaalisiin hallintopalveluihin. Toisena henkilönä esiintymistä ja muita kyberhyökkäyksiä varten on olemassa lukuisia vaihtoehtoja, jotka väärentävät toisen henkilön digitaalisen identiteetin. (Grassi, Garcia & Fenton 2020, luku 2.)

2.1 Digitaalisen identiteetin todentamisen malli

Grassin ja ym. (2020, luku 2) mukaan tietoturvaan ja digitaaliseen todentamiseen liittyvässä prosessissa on useita vaiheita ja osapuolia. Kuviossa 1 nähdään vasemmalla puolella ilmoittautumis-, valtakirja- ja elinkaaren hallintatoiminnot sekä identiteetin varmistus- ja todentamisprosessin eri vaiheet. Yleinen vuorovaikutusjärjestys näissä vaiheissa on seuraava:

1. Hakija hakee CSP:tä ilmoittautumisprosessin avulla.
2. CSP tarkistaa hakijan henkilöllisyyden. Jos todentaminen onnistuu, hakijasta tulee tilaaja.
3. Autentikaattorit, kuten salasanat tai muut todentamistiedot luodaan tilaajan ja CSP:n välille.
4. CSP säilyttää valtuustiedot, tilan ja rekisteröintitiedot, jotka kerätään valtuuskirjan voimassaolon aikana. Tilaaja ylläpitää omia autentikaattoreitaan.

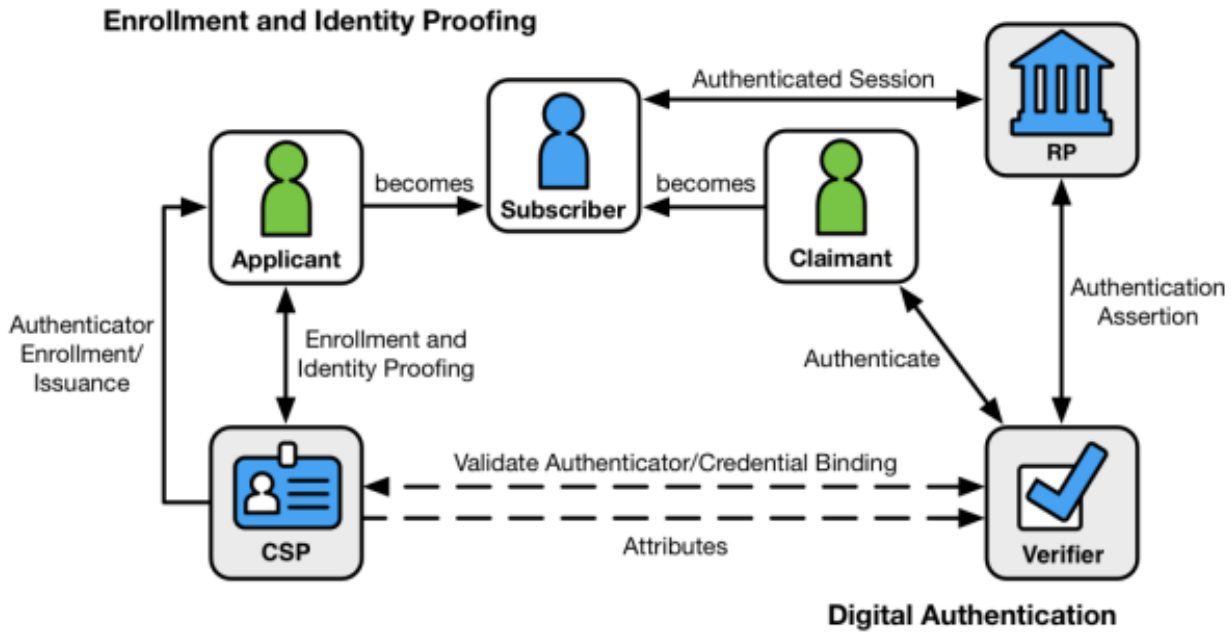


Figure 4-1 Digital Identity Model

Kuvio 1. Digitaallisen identiteetin malli (Grassi ym. 2020, luku 4.1)

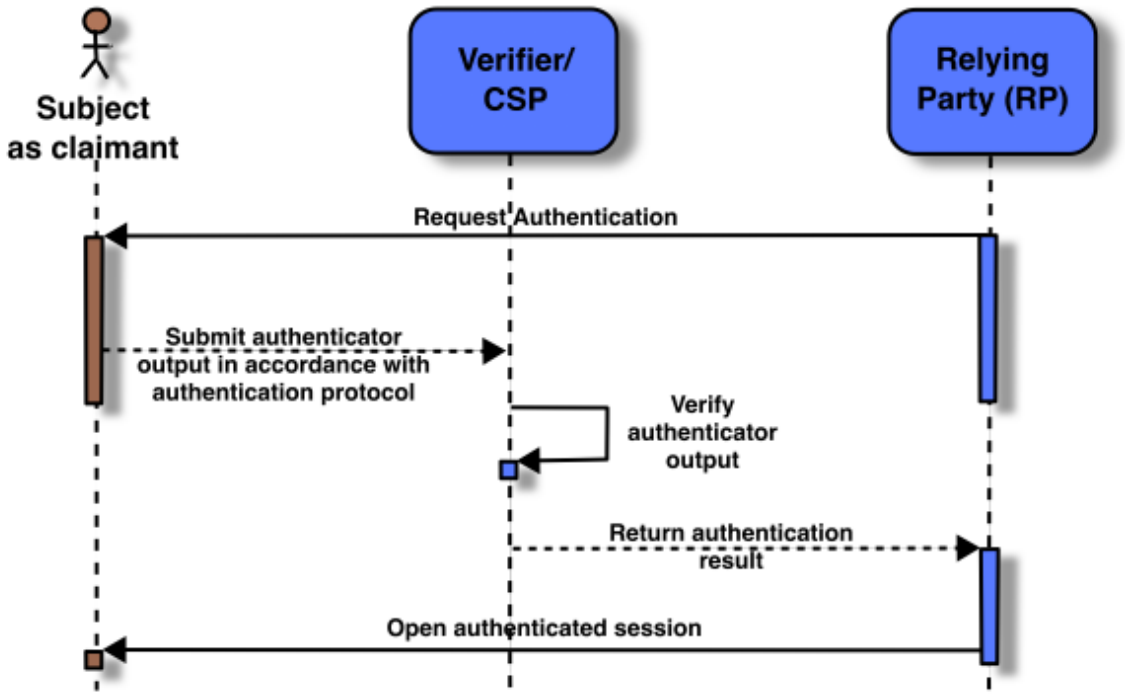
Grassin ym. (2020, luku 4.1) teoksen kuvion 1 oikealla puolella nähdään autentikaattorin käyttöön liittyvät toimijat ja vuorovaikutukset digitaalisen todentamisen aikana:

5. Hakija todentaa itsensä todentajalle käyttämällä autentikaattoriaan ja todentamisprotokollaa.
6. Todentaja vuorovaikuttaa CSP:n kanssa valtuustietojen vahvistamiseksi ja tarvittaessa hankkii lisätietoja vaatimuksen tekijältä.
7. CSP tai todentaja tarjoaa väitteen RP:lle, joka voi käyttää näitä tietoja valtuutuspäätöksen tekemiseen.
8. Tilaajan ja RP:n välillä muodostetaan suojattu ja todennettu istunto palvelun suorittamiseksi.

RP:n on pyydettävä tarvitsemansa attribuutit CSP:lta ennen palvelun todentamista. Joissakin tilanteissa todentajan ja CSP:n välillä voi olla viestintää valtuustietojen käsittelyssä. Tämä prosessi auttaa varmistamaan, että oikea henkilö saa pääsyn tarvittaviin palveluihin ja että henkilöllisyyden todistaminen tapahtuu turvallisesti ja luotettavasti. Valtaosa toimista perustuu autentikaattoreihin, valtuustietoihin ja niiden asianmukaiseen hallintaan. (Grassi ym. 2020, luku 4.1.)

2.2 Digitaalisen todentamisen prosessi

Grassin ym. (2020, 14) mukaan kuviossa 2 esitelty todentamisprosessi alkaa, kun hakija esittelee todentajalle todentamistiedot, jotka sisältävät autentikaattorin ja sen hallinnan. Nämä tiedot liittyvät henkilön vahvistettuun identiteettiin, ja ne tarkistetaan käyttäen tietyn tyyppistä todentamisprotokollaa. Kun nämä tiedot on vahvistettu, todentaja varmistaa, että hakijan valtuutustiedot ovat edelleen voimassa. Tämä tapahtuu yleensä vuorovaikutuksessa CSP:n kanssa. Todentajan ja hakijan välinen vuorovaikutus tässä protokollaprosessissa on erittäin tärkeää, kun mietitään järjestelmän yleistä turvallisuutta. Hyvin suunnitellut protokollat auttavat suojaamaan viestinnän eheyttä ja luottamuksellisuutta niin hakijan kuin todentajan välillä, niin itse todentamisprosessin aikana kuin sen jälkeenkin. Lisäksi nämä protokollat voivat auttaa rajoittamaan mahdollisia vahinkoja, joita hyökkääjä, joka yrittää esittäytyä lailliseksi todentajaksi voi aiheuttaa. Todentajassa olevat turvamekanismit voivat myös lieventää verkkohyökkäyksiä, joissa yritetään arvata matalan monimutkaisuuden salaisuuksia, kuten salasanoja tai PIN-koodeja. Tämä tapahtuu rajoittamalla hyökkääjän nopeutta tehdä useita todentamisyrityksiä tai hidastamalla virheellisiä yrityksiä. Tämä rajoitetaan yleensä pitämällä kirjaa epäonnistuneista yrityksistä ja asettamalla rajoituksia niiden määrälle, koska useimmat yritykset epäonnistuvat tällaisissa verkkohyökkäyksissä. (Grassi ym. 2020, 14.)



Kuvio 2. Digitaalisen todentamisen prosessi (Grassi ym. 2020, 14)

2.3 Digitaalisen todentamisen autentikaattorit ja todentamismenetelmät

Grassi ym. (2020, 12) määrittelevät todentamisjärjestelmien perusperiaatteen kolmen keskeisen tekijän varaan: Tieto, jonka käyttäjä tuntee, esimerkiksi salasana tai asia, joka käyttäjällä on kuten henkilötunnus tai salausavain sekä ominaisuus, joka käyttäjällä on kuten sormenjälki tai muut biometriset tiedot. He korostavat, että monivaiheinen todentaminen sisältää useamman kuin yhden näistä tekijöistä ja, että todentamisjärjestelmän vahvuus riippuu sisällytettyjen tekijöiden määrästä eli mitä enemmän tekijöitä sitä vahvempi järjestelmä. Grassi ym. (2020, 12) toteavat myös, että yleensä kahden tekijän käyttö riittää useimpien turvallisuusvaatimusten täyttämiseen. Digitaalisessa todentamisessa hakijalla on yksi tai useampi autentikaattori, joka on rekisteröity CSP:lle, ja jota käytetään hakijan henkilöllisyyden todentamiseen. Autentikaattorit sisältävät salaisuuksia, joita hakija voi käyttää osoittaakseen olevansa laillinen käyttäjä, ja hakijan on todistettava hallitsevansa yksi tai useampi näistä todentamismenetelmistä. (Grassi ym. 2020, 12.)

Grassin ym. (2020, 13–14) mukaan autentikaattorit voivat perustua joko julkisiin avainpareihin, eli epäsymmetrisiin avaimiin, tai jaettuihin salaisuuksiin, eli symmetrisiin avaimiin. Julkisen avainparin muodostavat julkinen avain ja siihen liittyvä yksityinen avain, jossa yksityinen avain säilytetään autentikaattorissa ja käytetään todistamaan käyttäjän hallitsevan kyseistä avainta. He kuvaavat, miten autentikaattori voi käyttää kantajan julkisen avaimen sertifikaattia henkilöllisyyden vahvistamiseen, ja miten jaetut salaisuudet, kuten symmetriset avaimet tai käyttäjän muistiinpanemat salasanat ja PIN-koodit, tallennetaan autentikaattoriin. Grassi ym. (2020, 13–14) korostavat, että symmetriset avaimet säilytetään yleensä käyttäjän hallitsemissa laitteissa tai ohjelmistoissa, kun taas salasanat ovat käyttäjän omassa muistissa. He huomauttavat, että useimmat käyttäjät valitsevat helposti muistettavia salasanoja, mikä tekee niistä haavoittuvampia erityisesti ilman asianmukaista suojausta. Grassi ym. (2020, 13–14) toteavat, että autentikaattorit sisältävät aina jonkin salaisuuden ja että perinteiset todentamistekijät, kuten fyysinen ajokortti eivät suoraan sovellu digitaaliseen todentamiseen. He mainitsevat myös biometriset ominaisuudet, kuten kasvonpiirteet, sormenjäljet ja iiriskuvioinnit ainutlaatuisina fyysisinä piirteinä, jotka voidaan käyttää henkilöllisyyden varmistamiseen digitaalisessa todentamisjärjestelmässä. Grassi ym. (2020, 13–14) korostavat, että digitaalisen todentamisjärjestelmän turvallisuutta voidaan parantaa käyttämällä erilaisia tekijöitä ja suojaamalla niitä asianmukaisesti. (Grassi ym. 2020, 13–14.)

2.3.1 Muistiin sitoutunut salasana

Burrin, Choongin, Dankerin, Fentonin, Garcian, Grassin, Greenen, Lefkovitzin, Newtonin, Perlnerin, Regenscheidin, Richerin ja Theofanosin (2020, luku B.4.1.2) mukaan muistiin sitoutuneet autentikaattorit ovat yleisimmin käytetty autentikointityyppi. Heidän mukaansa tilaajien on muistettava salasanat, tunnuslauseet ja PIN-koodit, ja termi "muistissa oleva salaisuus" viittaa näihin kaikkiin. Nämä ulkoa tallennetut salaisuudet ovat yleisiä vähäturvallisissa tilanteissa. Turvallisuuden lisäämiseksi käytetään kaksivaiheista strategiaa, joka jakaa turvallisen hajautusvastuun autentikaattoreille ja asettaa vähimmäisstandardeja online-hyökkäyksiltä suojautumiselle samalla kun tunnustetaan offline-hyökkäysten mahdollisuus. Autentikaattoreiden tulee turvallisesti tiivistää oppimansa salaisuudet, joihin voi sisältyä salaisen arvon käyttö tai iteratiivinen hajautus suolalla. PIN-koodit, tunnuslauseet ja salasanat ovat esimerkkejä ulkoa opitusta salaisuuksista. Vaikka termejä käytetään joskus vaihtokelpoisesti, salalauseet ovat yleensä pidempiä kuin salasanat ja sisältävät välilyöntejä. PIN-koodit toimitetaan käyttäjille numeerisessa muodossa viestintäpalveluiden tarjoajien tai autentikaattorien toimesta. Ne generoidaan satunnaisesti, mikä takaa, että niiden entropiataso on korkeampi verrattuna käyttäjien itse valitsemiin salaisuuksiin. (Burr, Choong, Danker, Fenton, Garcia, Grassi, Greene, Lefkovitz, Newton, Perlner, Regenscheid, Richer & Theofanos 2020, luku B.4.1.2.)

2.3.2 Hakusalaisuus

Burr ym. (2020, luku B.4.1.3) selostavat, että hakusalaisuudet ovat eräänlaisia salaisuuksia, joita Credential Service Provider myöntää tilaajilleen ja, jotka on suunniteltu yhtä onnistunutta todentamista varten. Nämä salaisuudet voidaan ymmärtää fyysisinä esineinä, kuten kortteina tai muina välineinä, jotka sisältävät salaisuudet ja ovat käyttäjän hallussa. Hakusalaisuudet ovat erityisen hyödyllisiä tilanteissa, joissa ensisijainen todentamismenetelmä on vaarantunut, esimerkiksi kadonnut tai varastettu. Ne tarjoavat vaihtoehtoisen tavan varmistaa käyttäjän henkilöllisyys. Hakusalaisuudet ovat kertakäyttöisiä ja niitä tulee suojata huolellisesti. Niiden jakelu tapahtuu joko henkilökohtaisesti, postitse tai molemminpuolista todentamista vaativan suojatun istunnon aikana. Säilytys tapahtuu yleensä turvallisesti tilaajan kiinteistössä. Online-jakelun tulisi tapahtua suojattujen kanavien kautta, jotka vaativat AAL2:n tai korkeamman todentamistason. Vaikka hakusalaisuuksien kantaminen lisää varkauden tai katoamisen riskiä, se mahdollistaa myös nopean löytämisen. Todentamisen vastuulla on salaisuuksien turvaaminen, ja vaikka matalan entropian salaisuuksia sallitaankin, korkean entropian käyttöä suositellaan erityisesti varmuuskopioiden

todentamisessa. Suosituimpia hakusalaisia autentikaattoreita ovat suojatun satunnaisbitti-generaattorin tuottamat painetut salaisuuksien luettelot, jotka voidaan ryhmitellä helpomman lukemisen takaamiseksi. (Burr ym. 2020, luku B.4.1.3.)

2.3.3 Kaistan ulkopuolinen laite

Burr ym. (2020, luku B.4.1.4) mukaan kaistan ulkopuoliset autentikaattorit ovat laitteita tai välineitä, joita käytetään todentamisessa erillisen yksityisen viestintäkanavan kautta, joka eroaa pääasiallisesta todennettavasta kanavasta. Tämän tyyppisten autentikaattorien tarkoituksena on varmistaa, että hakija omistaa tietyn fyysisen laitteen tai välineen, joka liittyy todentamiseen. Ne ovat keskeisiä monissa todentamisprosesseissa, mutta niiden käyttö vaatii tiettyjen seikkojen huomioimista, kuten laitteiden kytkemistä pois päältä ilman uudelleen rekisteröintiä tai usean laitteen käyttämistä yhteen todentamiseen. Burr ym. (2020, luku B.4.1.4) korostavat, että VoIP-pohjaisia puhelinjärjestelmiä ja sähköpostipalveluita ei voida käyttää kaistan ulkopuolisessa todentamisessa ja on tärkeää, että kaistan ulkopuoliset laitteet korreloidaan tietyn istunnon kanssa. He esittävät kaksi lähestymistapaa: joko molemmat kanavat näyttävät salaisuuden vertailua varten tai salaisuus lähetetään ensisijaisen kanavan kautta ja palautetaan toissijaisen kanavan kautta. Lisäksi he painottavat, että kaistan ulkopuolisen laitteen turvallinen ja yksilöllinen todentaminen on välttämätöntä, ja autentikaattoria ei tarvitse fyysisesti erottaa todentamispaikasta, kunhan käytetään erilaisia viestintäreittejä. Burr ym. (2020, luku B.4.1.4) mainitsevat myös, että suosittu kaistan ulkopuolinen todentamistekniikka on satunnaisen salaisuuden lähettäminen tilaajan matkapuhelimeen, mutta tämä menetelmä sisältää tietoturvapuutteita, kuten puhelinnumeron uudelleenmäärityksen riskin ja SS7-haavoittuvuudet. He suosittelevat vahvaa laitesidontaa ja päästä päähän -salausta turvallisempina vaihtoehtoina. (Burr ym. 2020, luku B.4.1.4.)

2.3.4 Yksivaiheinen One-Time-Password -laite

Burr ym. (2020, luku B.4.1.5) esittävät yksivaiheisen OTP-laiteen olevan väline, jonka tilaaja omistaa ja joka tuottaa kertakäyttöisiä salasanoja. Tämä autentikaattori voi olla joko erillinen fyysinen laite tai ohjelmistosovellus, joka toimii yleiskäyttöisessä laitteessa, kuten älypuhelimessa, ja edustaa "jotain, mitä sinulla on" -todentamistekijää. Käyttäjä näyttää nämä kertakäyttöiset salasanat laitteeltaan ja syöttää ne manuaalisesti todentamisprosessissa. Yksivaiheiset OTP-laitteet voivat

tuottaa aikapohjaisia tai ei-aikapohjaisia salasanoja, ja onnistuneen todentamisen jälkeen autentikaattoreiden tulee päivittää tilansa. Aikapohjaiset OTP-laitteet vaativat synkronoinnin tilaajan ja varmentajan kellojen välillä. Koska näiden laitteiden tuloste syötetään manuaalisesti, ne luokitellaan usein salauslaitteiksi. OTP-laitteet keskittyvät tietojenkalastelusuojaukseen eivätkä ne ole vahvoja autentikaattoreita esiintymisen suhteen. Markkinoilla on saatavilla useita kaupallisia OTP-laitteita, sekä ohjelmisto- että laitteistomuodossa. Initiative for OATH on toimialaryhmä, joka kannustaa OTP-autentikaattoreiden käyttöönottoon. (Burr ym. 2020, luku B.4.1.5.)

2.3.5 Monivaiheinen One-Time-Password -laite

Burr ym. (2020, luku B.4.1.6) toteavat samoin kuin yksivaiheiset OTP-laitteet myös monivaiheiset OTP-laitteet aktivoidaan syöttämällä muistiin tallennettu salaisuus tai esittämällä biometrinen tieto kertaluonteisen salasanan saamiseksi. Monivaiheinen OTP-laite edustaa jotain, mitä omistat -todentamistekijää, ja sen lukitus avataan joko identiteetin tai tiedon perusteella. Nämä laitteet kohtaavat samankaltaisia haasteita kuin yksivaiheiset OTP-laitteet, kuten mahdollisuuden antaa väärän tuloksen arvaushyökkäyksiä estäväksi tai virhesignaalin, kun väärä salaisuus syötetään. Erityisesti biometristen tietojen käyttöön perustuvissa OTP-laitteissa voi esiintyä suurempaa väärien hylkäysten määrää, mikä lisää virheiden vaikutusta tarkoituksenmukaisissa tuloksissa. Tämän vuoksi on tärkeää tarjota varmuuskopiointisuunnitelmia, kuten salainen koodi tai vaihtoehtoinen autentikaattori biometrisen todentamisen toimimattomuuden varalta. (Burr ym. 2020, luku B.4.1.6.)

2.3.6 Yksivaiheinen salausohjelmisto

Burr ym. (2020, luku B.4.1.7) kuvaavat yksitekijäisen salausohjelmistotodentajan, joka koostuu salaisesta salausavaimesta ja siihen liittyvistä ohjelmistoista tallennettuna ohjelmiston käyttämälle tietovälineelle. Tämän todentajan käyttöön liittyy keskeisesti kyky osoittaa pääsy sulautettuun avaimeen. Tämä eroaa OTP-laitteista siinä, että tuloste tuotetaan suoraan sovellukselle, mikä mahdollistaa korkeamman entropian tulosteet, mutta ilman haaste-vastausjärjestelmän lisäturvallisuutta. Esimerkkinä tällaisesta todentajasta on asiakkaan X.509-sertifikaatti TLS-protokollassa, joka sisältää turvallisesti säilytetyn yksityisen avaimen ja julkisen avaimen. Tämäntyyppinen autentikaattori ei välttämättä vaadi laajasti tunnustettuja juurivarmenneviranomaisia julkisen avaimen

yhdistämiseen tilaajaan, vaan yhteys voidaan muodostaa varmenneviranomaisten tai suoran assosioinnin kautta tarjoten näin yksityiskohtaisen kuvauksen yksitekijäisen salausohjelmistotodentajan toiminnasta ja sen merkityksestä todentamisprosessissa. (Burr ym. 2020, luku B.4.1.7.)

2.3.7 Yksivaiheinen kryptografinen laite

Burr ym. (2020, luku B.4.1.8) toteavat yksivaiheisten salauslaitteiden olevan verrattavissa yksitekijäisiin ohjelmistoautentikaattoreihin, mutta niissä yksityinen avain on lukittu laitteistoon ja sitä ei voi viedä pois laitteesta säännöllisen käytön aikana. Tämä tarkoittaa, että todentamiseen liittyvät salaustehtävät suoritetaan laitteiston toimesta. Yksivaiheisia salauslaitteita on monenlaisia, kuten laitteisto-TPM, älykortit, USB-pohjaiset laitteet ja FIDO U2F -todentajat. Näillä laitteilla on erilaisia liitäntävaihtoehtoja, kuten käyttäjäpäätteisiin liitettävät ja langattomat esimerkiksi NFC tai USB. Koska monet näistä laitteista tarjoavat erilaisia toimintatiloja, on tärkeää tunnistaa ja valita sopiva tila käyttöön. Esimerkiksi FIDO U2F -todentajat voivat tukea sekä vähemmän turvallista perinteistä kertakäyttöisen salasanan tilaa että suojattua haaste-vastaustilaa, mikä tekee niistä monipuolisen valinnan erilaisiin turvallisuusvaatimuksiin. (Burr ym. 2020, luku B.4.1.8.)

2.3.8 Monivaiheinen kryptografinen ohjelmisto

Burr ym. (2020, luku B.4.1.9) näkevät monivaiheisten kryptografisten ohjelmistoautentikaattoreiden olevan samankaltaisia yksivaiheisten kanssa paitsi, että niissä käyttäjän on syötettävä salaisuus yksityisen avaimen käyttöön todentamista varten. Nämä monivaiheiset autentikaattorit ovat omaisuutta, joiden aktivoiminen edellyttää tietoa. Haasteena näissä autentikaattoreissa on määrittää, onko monivaiheinen todentaminen todella suoritettu. On mahdollista, että yhteistyöhön sitoutunut tilaaja purkaa ja tallentaa salatun yksityisen avaimen, mikä alentaa todentamisprosessin yksivaiheiseksi. Tämä vähentää tilaajan tarvitsemaa työmäärää ilman autentikaattorin tietämystä tai hyväksyntää sillä salattu yksityinen avain on tilaajan ohjelman käytettävissä. Nämä autentikaattorit toimivat tyypillisesti paremmin tietyillä alustoilla erityisesti mobiililaitteilla verrattuna yleiskäyttöisiin laitteisiin, koska mobiililaitteissa on vähemmän mahdollisuuksia purkaa ja tallentaa yksityisiä avaimia. (Burr ym. 2020, luku B.4.1.9.)

2.3.9 Monivaiheinen salauslaite

Burrin ym. (2020, luku B.4.1.10) mukaan myös monivaiheiset salauslaitteiden autentikaattorit vaativat samankaltaisesti kuin yksivaiheiset laitteistoautentikaattorit, että käyttäjä syöttää muistiin jääneen salaisuuden tai varmentaa biometrisen tiedon. Nämä monivaiheiset autentikaattorit ovat omaisuutta, jota käytetään tunnistamalla käyttäjä tai varmentamalla jokin joka käyttäjällä on. Aktivointiprosessi käsittää yksityisen avaimen salauksen purkamisen tai sen valmistamisen todentamista varten. Isäntäpäätepisteet, jotka edellyttävät korkeaa turvallisuutta, tai laitteen sisäiset aktivointitekijät, kuten laitteen muistiin tai biometrisiin tietoihin sidottu salausavain ovat yleisiä tämäntyyppisissä autentikaattoreissa. Useiden epäonnistuneiden yritysten jälkeen aktivointitekijöitä voidaan rajoittaa, ja todentaja voi tallentaa tai välittää nämä tiedot edelleen. Toisin kuin OTP-laitteet kryptografiset autentikaattorit on suoraan liitetty päätepisteeseen eivätkä vaadi käyttäjän manuaalista syöttöä todentamistulosten osalta. Ne tukevat useita toimintoja, kuten todentamisvastauksia ja kertakäyttöisiä salasanoja. Puolustusministeriön CAC ja Yhdysvaltain hallituksen PIV-todentajat ovat esimerkkejä monivaiheisten kryptografisten autentikaattoreiden käytöstä. Ryhmään kuuluu myös muita älykorttiautentikaattoreita, kuten Virossa käytettävä e-asukaskortti. FIDO UAF -todentajien tapaan myös monivaiheiset salauslaitteet voidaan integroida suoraan päätepisteisiin. (Burr ym. 2020, luku B.4.1.10.)

2.4 Digitaalisen todentamisen haasteet

Digitaalisen todentamisen teknologian kehittyminen on vastaus kasvaviin tietoturva- ja yksityisyysvaatimuksiin, ja se integroituu entistä syvemmin päivittäiseen elämäämme ja liiketoimintaprosesseihimme, mutta samalla se tuo mukanaan useita haasteita. Nämä haasteet ovat moninaisia ja ulottuvat laajalle eri näkökulmista. Yhtenä keskeisenä haasteena on turvallisuuden varmistaminen, joka sisältää vahvat salausmenetelmät ja tietomurtojen ehkäisyn varmistamalla, että arkaluonteiset tiedot säilyvät suojattuina. Toinen merkittävä haaste on käyttäjien yksityisyyden suojaaminen erityisesti henkilökohtaisten tunnistetietojen kuten sormenjälkien tai kasvojentunnistustietojen osalta. Järjestelmän käytettävyydellä on myös suuri merkitys; sen tulee olla helppokäyttöinen ja saavutettava eri käyttäjäryhmille. Teknologian nopean kehityksen ja digitalisaation laajentumisen myötä tulevat myös skaalautuvuuden ja sopeutumiskyvyn haasteet. Lisäksi lainsäädännölliset ja eettiset kysymykset, kuten tietosuojamääräykset ja käyttäjän suostumuksen hallinta ovat keskeisiä tekijöitä, jotka vaikuttavat digitaalisen todentamisen kehitykseen ja muotoutumiseen.

Morrow (2020) käsittelee nykyisten digitaalisten identiteettijärjestelmien haasteita kuvaten niitä lähtökohtaisesti naiiveiksi. Morrowin (2020) mukaan nämä järjestelmät pyrkivät luomaan digitaalisen esityksen yksilön henkilöllisyydestä erilaisin varmistusmenettelyin, kuten henkilöllisyyspapereiden tutkiminen ja petostentorjuntatoimenpiteiden suorittaminen. Hän huomauttaa, että vaikka tavoitteena on erottaa lailliset käyttäjät hakkereista niin prosessi kohtaa useita esteitä. Esimerkiksi UK Verify -järjestelmän ongelmat osoittavat, että digitaalisen identiteetin saaminen voi olla vaikeaa tai jopa mahdotonta johtuen tiukoista vaatimuksista luottamustason saavuttamiseksi. Morrow (2020) nostaa esiin myös synteettisten henkilöllisyyksien ja syvävääreennösten käytön, jotka tekevät digitaalisista tunnuksista epävarmoja ja alttiita petoksille. Lisäksi hän mainitsee, että jokaisen verkkopalvelun erillisten identiteettien ylläpito johtaa hallitsemattomaan verkkotilien ylimäärään, mikä vaikeuttaa hallinnointia ja lisää petosten riskiä. Morrow (2020) korostaa, että nykyiset digitaalisen tunnistuksen järjestelmät eivät tue suvereniteetin ajatusta sillä ne eivät ole riittävän joustavia hallitsemaan henkilöllisyyden valvontaa. Hänen mukaansa nämä puutteet vaativat digitaalisen tunnistamisen uudelleensuunnittelua, joka ylittää staattisen henkilöllisyyden todentamisen rajoitukset ja tarjoaa dynaamisemman, turvallisemman ja jatkuvan digitaalisen olemassaolon ilmaisevan järjestelmän. (Morrow 2020.)

3 Monivaiheisen todentamisen teknologia

Monivaiheinen todentaminen, joka tunnetaan tutummin nimellä MFA on tietoturvan peruskonsepti, joka on myös kasvattanut merkitystään merkittävästi digitaalisen aikakauden aikana. Se on käytäntö, jossa käyttäjän todentaminen ja pääsy tiettyihin järjestelmiin, sovelluksiin tai palveluihin edellyttää useiden eri todentamistekijöiden eli tunnistautumistapojen onnistunutta läpäisyä. Tämä lisää tietoturvaa huomattavasti verrattuna perinteiseen yksivaiheiseen tai kaksivaiheiseen todentamiseen, jossa käytetään yhtä tai kahta tekijää yleensä salasanaa ja kertakäyttöistä koodia.

Vaikka kyberrikollisuuden täydellinen estäminen on mahdotonta, on olemassa helppoja asioita, joiden avulla voidaan vähentää merkittävästi todennäköisyyttä, että joudutaan sen uhriksi uudelleen. Aina kun mahdollista tulisi käyttää monivaiheista todentamista erityisesti arkaluontoisten tietojen, kuten ensisijaisen sähköpostiosoitteen, pankkitilin tietojen ja sairaustietojen osalta. Vaikka monet organisaatiot tarjoavat MFA:n valinnaisena ominaisuutena, joka voidaan ottaa käyttöön, henkilön on tehtävä itse aloite käyttääkseen sitä, mutta jotkut yritykset onneksi määräävät sen

käytön pakollisena. Lisäksi kannattaa harkita aina kahdesti palvelua, jolloin tarjolla tietojen turvaksi ja suojaamiseksi on vain salasana MFA:n sijasta ennen kuin sinne annetaan tietoja. (Back to basics: Multi-factor authentication (MFA) 2023.)

3.1 Historia ja kehitys

Digitalisaatiolla on Andreevin, Bezzateevin, Koucheryavyn, Mikkosen, Mäkitalon & Ometovin (2018, luku 1) mielestä syvällinen vaikutus nyky-yhteiskunnan jokaiseen osa-alueeseen. He näkevät todentamisen olevan tärkeä keino tämän prosessin turvaamisessa. Se sisältää laajan valikoiman aiheita, jotka liittyvät tulevaisuuteen, jossa kaikki on linkitetty kuten viestintä, online-maksut, käyttöoikeuksien hallinta ja paljon muita. Kuviossa 3 nähdään todentamisjärjestelmien kehitys, joka on alkanut yksivaiheisesta todentamisesta ja jatkunut aina monivaiheiseen todentamiseen asti käymällä välissä kaksivaiheisen todentamiseen aikakauden läpi. Erityisesti monivaiheista todentamista odotetaan käytettävän ihmisten ja asioiden väliseen vuorovaikutukseen, koska se mahdollistaa nopean, yksinkertaisen ja luotettavan todentamisen, kun käyttäjä haluaa käyttää palvelua, mutta siihen liittyy tietoturvariskejä palveluntarjoajan ja käyttäjän näkökulmista. Joustavamman todentamisen mahdollistamiseksi ehdotetaan juuri monivaiheisen todentamisen -järjestelmää, joka perustuu Shamirin salaisen jakamisen menetelmän sisällä olevaan käänteiseen Lagrange-polynomiin. Tämä menetelmä käsittelee käyttäjän todentamisen tilanteissa, joissa jotkin vaatimukset puuttuvat tai ovat virheellisiä. Arkkitehtuuri mahdollistaa puuttuvien komponenttien hyväksymisen paljastamatta arkaluonteisia biometrisiä tietoja varmennusorganisaatiolle todentaessa käyttäjää. (Andreev, Bezzateev, Koucheryavy, Mikkonen, Mäkitalo & Ometov 2018, luku 1.)

Kuvio 3. Todentamismenetelmien kehitys (Andreev ym. 2018, luku 1)

Myös Boonkrong (2021, luku 6) pitää monivaiheista todentamista laajennuksena ja parannuksena kaksivaiheisesta todentamisesta. Monivaiheinen todentaminen on todentamismenettely, joka

käyttää kahta tai mieluiten useampaa todentamistekijää. Se on tällä hetkellä hyväksytty ja sitä pidetään käytännössä standardina kaikille korkeaa turvallisuutta vaativille järjestelmille. Uusien tietojärjestelmien kehityksen seurauksena todentamisjärjestelmille on useita mahdollisuuksia, mutta myös haasteita ja mahdollisia ongelmia. On väitetty muun muassa, että lisäelementtien lisääminen henkilöllisyyden todentamisprosessiin lisää todentamisen luottamusta ja turvallisuutta nousujohteisesti. Vaikka kulunvalvontamenetelmä on nyt turvallisempi kaksivaiheisen todentamisen ansiosta, on silti kiehtovaa tutkia, kuinka vankempaa todentamisjärjestelmää voidaan käyttää monivaiheisen todentamisen yhteydessä. Koska identiteetin vahvistamiseen tarvitaan enemmän elementtejä käytettäessä monivaiheista todentamista, kulunvalvontajärjestelmät voidaan tehdä yleisesti turvallisemmiksi. Mutta on tärkeää muistaa, että käytettävyys ja mukavuus ovat edelleen ongelmia, jotka vaativat huomiota. Järjestelmän suojaamiseksi tunkeilijoilta on kuitenkin otettava käyttöön tehokkaampi todentamisprosessi. Tulevaisuudessa mahdollisesti hyödynnettäviä monivaiheisia todentamisprotokollia voidaan suunnitella ja rakentaa useiden todentamistekijätyyppien saatavuudella. (Boonkrong 2021, luku 6.)

3.2 Toimintaperiaate

Yasarin (2023) mukaan monivaiheinen todentaminen on prosessi, joka vaatii useita todentamismenetelmiä eri tunnisteluokista käyttäjän henkilöllisyyden vahvistamiseksi sisäänkirjautumisen tai muun tapahtuman yhteydessä. Hän selittää, että biometristen varmennustekniikoiden avulla monivaiheinen todentaminen yhdistää aiemmin mainitut kaksi tai mieluiten useampia riippumattomia tunnistetietoja: käyttäjän henkilöllisyyden, hallussaan olevat suojaustunnukset ja tietämänsä salasanat. Yasarin (2023) mukaan monivaiheisen todentamisen tavoitteena on vaikeuttaa luvattoman henkilön pääsyä kohteeseen, kuten fyysiseen paikkaan tai tietojärjestelmään. Hän korostaa, että vaikka yksi tunnistetekijöistä vaarantuisi hyökkääjän on silti voitettava useita esteitä päästäkseen kohteeseen. Yasar (2023) mainitsee, että monivaiheiset todentamisjärjestelmät luottivat aiemmin usein kaksivaiheiseen todentamiseen, mutta nykyään toimittajat viittaavat monivaiheiseen todentamiseen yhä useammin, kun tarvitaan kaksi tai useampia tunnistetietoja kyberhyökkäysten riskin vähentämiseksi. Hän painottaa monivaiheisen todentamisen merkitystä osana identiteetin ja pääsynhallintajärjestelmiä huomauttaen, että tavalliset käyttäjätunnukset ja salasanat eivät yksinään estä hakkerointia, mikä voi aiheuttaa yrityksille suuria taloudellisia menetyksiä. Yasar (2023) mainitsee myös brute force -hyökkäysten riskin, joissa pahantahtoiset toimijat käyttävät automatisoituja järjestelmiä yrittäessään lukuisia käyttäjätunnus- ja salasanayhdistelmiä. Lopuksi

hän toteaa, että yritysten suojautumiskeinoihin kuuluu tilin lukitseminen epäonnistuneiden kirjautumisyritysten jälkeen, mutta huomauttaa, että hakkerit keksivät jatkuvasti uusia tapoja järjestelmiin tunkeutumiseen ja kyberhyökkäysten käynnistämiseen. (Yasar 2023.)

3.3 Edut ja haitat

Yasarin (2023) mukaan monivaiheisen todentamisen käyttöönotto laitteiston ja ohjelmiston kautta on tehty järjestelmien ja sovellusten suojatun pääsyn vahvistamiseksi päämääränä käyttäjien digitaalisten tapahtumien eheyden ja heidän henkilöllisyytensä varmistaminen. Hän huomauttaa, että yksi monivaiheisen todentamisen haittapuolista on, että käyttäjät voivat vaihtaa salasanojaan ja henkilökohtaisia tunnuksiaan, mikä saattaa johtaa siihen, että he unohtavat usein vastaukset henkilöllisyyttä vahvistaviin henkilökohtaisiin kysymyksiin. Yasar (2023) korostaa, että monivaiheisella todentamisella on myös monia muita etuja ja haittoja, jotka tulee ottaa huomioon sen käytön yhteydessä. (Yasar 2023.)

Yasarin (2023) mukaan monivaiheinen todentaminen tarjoaa lukuisia etuja tietoturvan kannalta. Se lisää henkilökohtaisen tunnistautumisen, ohjelmiston ja laitteiston tietoturvakerroksia. Hän mainitsee, että monivaiheisessa todentamisessa voidaan käyttää satunnaisesti generoituja salasanoja, jotka ovat vaikeasti murrettavia ja toimitetaan puhelimiin reaaliajassa, ja että tämä lähestymistapa voi vähentää tietoturvaloukkauksia lähes sataprosenttisesti verrattuna pelkkien salasanojen käyttöön. Yasarin (2023) mukaan monivaiheisen todentamisen helppo käyttöönotto tekee siitä käyttäjille vaivatonta. Lisäksi se mahdollistaa yrityksille pääsyn rajoittamisen sijainnin tai ajan perusteella ja tarjoaa skaalautuvan kustannusrakenteen, joka sopii eri kokoisille organisaatioille. Yasar (2023) korostaa, että monivaiheisen todentamisen avulla yritykset voivat asentaa järjestelmiä, jotka aktiivisesti hälyttävät epäilyttävistä kirjautumisyrityksistä, parantaen näin tietoturvatoimia ja reagointia. Hän mainitsee myös adaptiivisen todentamisen, joka auttaa organisaatioita mukautumaan muuttuviin työolosuhteisiin erityisesti, kun yhä useammat työntekijät suosivat etätyötä. Lisäksi Yasar (2023) toteaa, että monivaiheinen todentaminen auttaa noudattamaan HIPAA-standardeja, jotka rajoittavat herkkien tietojen, kuten yksityisten lääketieteellisten tietojen, pääsyn vain hyväksyttyyn ja rajoitettuun käyttöön. (Yasar 2023.)

Yasarin (2023) mukaan monivaiheiseen todentamiseen liittyvät erilaiset haasteet. Hän mainitsee, että tekstiviestikoodien vastaanottamiseen tarvittava puhelin on keskeinen osa monivaiheista todentamisprosessia, mutta puhelimet ja laitteistotunnukset voivat olla alttiita varkaudelle tai katoamiselle. Lisäksi kun käytetään biometrisiä tietoja, kuten sormenjälkiä, monivaiheisessa todentamisessa, on tärkeää olla tietoinen niiden potentiaalisista heikkouksista. Yasar (2023) huomauttaa, että vaikka biometriset tiedot tarjoavat lisäsuojaa, ne eivät ole erehtymättömiä ja väärät positiiviset tai negatiiviset tulokset ovat mahdollisia, mikä voi johtaa virheelliseen tunnistukseen tai oikeutetun pääsyn estymiseen. Kolmantena haasteena hän mainitsee verkko- tai internetkatkokset, jotka voivat häiritä vahvistusprosessia ja aiheuttaa sen epäonnistumisen. Yasar (2023) korostaa, että monivaiheisten todentamisjärjestelmien jatkuvaa päivitystä ja parantamista on tärkeää ylläpitää hakkereiden murtautumisyritysten torjumiseksi. Tämä jatkuva parannustyö on hänen mukaansa välttämätöntä sekä makrotaloudellisen rahoitusavun tehokkuuden ylläpitämiseksi että arkaluonteisten tietojen ja järjestelmien turvallisuuden varmistamiseksi. (Yasar 2023.)

3.4 Todentamistekijät

Boonkrong (2021, 139) käsittelee digitaalisen todentamisen eri todentamistekijöitä, jotka ovat keskeisiä henkilön henkilöllisyyden vahvistamisessa monivaiheisessa todentamisessa. Hän mainitsee, että kaksivaiheisissa todentamisjärjestelmissä yhdistetään kaksi elementtiä useista luokista, mutta monivaiheiseen todentamiseen tarvitaan useampia kuin kaksi tekijää. Boonkrong (2021, 139) erittelee nämä tekijät neljään tyyppiin: jotain, mitä tiedät (kuten salasana), jotain, mitä sinulla on (esimerkiksi turvatunnus tai laite), jotain, mitä olet (kuten biometriset tiedot), ja jotain, mitä sinä prosessoit. Hän korostaa, että näiden eri tekijöiden yhdistäminen lisää todentamisen turvallisuutta ja monipuolistaa tietoturvamenetelmiä. (Boonkrong 2021, 139.)

Nykyään ammattilaiset käyttävät jopa viittä erilaista todentamistekijää nykyisessä digitaalisessa tietoturvaympäristössä. Näitä monenlaisia todentamistekijöitä, joita käyttäjä voi tarjota tunnistamisen todentamiseksi voi olla lisäksi jotain missä ja milloin olet. (Two-Factor Authentication (2FA) n.d.)

3.4.1 Tietotekijä

Tietopohjaisen todentamistekijän perusta on vain käyttäjän tiedossa oleva tieto kuten PIN-koodit, salasanat ja vastaukset turvakysymyksiin kuten isäsi nimi tai lempinimesi lapsena. Tämän tyyppinen todentaminen on edullinen, erittäin säädettävissä ja antaa käyttäjille mahdollisuuden valita monimutkaisia henkilökohtaisia tietoja, joita heidän mielestään ulkopuolisten olisi vaikea tulkita. Se tarjoaa myös äärettömän määrän helposti nollattavia kirjain- ja numeroyhdistelmiä. Sen haittoja ovat kuitenkin se, että käyttäjät voivat turhautua, jos he unohtavat tärkeitä tietoja, kirjalliset valtuustiedot voidaan varastaa, henkilökohtaisia tietoja voi löytyä julkisista tietueista tai sosiaalisessa mediassa ja käyttäjät joutuvat todennäköisemmin tietojenkalasteluhuijausten uhriksi, jossa he voivat vahingossa paljastaa arkaluonteisia tietoja. (What Is MFA? n.d.)

3.4.2 Omistustekijä

Hallussapitoon perustuvat todentamistekijät eli omistustekijät käyttävät yksilön tunnistamisen varmistamiseen konkreettisia esineitä, jotka käyttäjän on esitettävä saadakseen käyttöoikeuden. Tokenit ja kaukosäätimet, pankkikortit, viranomaistunnukset, älypuhelinsovellukset kuten Duo Push kulunvalvontaan, ja jopa FIDO2 turva-avaimet kuuluvat tähän luokkaan. Nämä hallussapitoon perustuvat työkalut tarjoavat laajan valikoiman etuja; niiden hinta ja kehittyneisyys voivat myös vaihdella merkittävästi aina erittäin kalliista ja turvallisista ratkaisuista edullisempiin sekä yksinkertaisempiin malleihin. Ne ovat turvallisimpia saatavilla olevia todentamistekniikoita, koska ne tarjoavat fyysisen suojakerroksen ja ne on usein tehty kestämään tietojenkalasteluhyökkäystä. Vaikka näillä konkreettisilla tokeneilla on etuja, niiden pienen koon ansiosta ne on helppo hävittää ja ne voivat rikkoutua, jos niitä ei käsitellä huolellisesti, ja halvemmissa malleissa on riski valmistusvirheistä. Kuluttajille voi aiheutua suurta harmia siitä, että joidenkin hallussapitoon perustuvien laitteiden vaihtaminen voi olla vaikeaa ja kallista. (What Is MFA? n.d.)

3.4.3 Luontaisuustekijä

Luontaisuustekijät eli ihmisen biometrisiin tietoihin perustuvat todentamistekijät todentavat henkilön hänen biologisten ominaisuuksiensa perusteella, mikä estää fyysisten esineiden tai sitoutuneen tiedon tarpeen. Luomalla yhteyden fyysisen ominaisuuden ja todentamisjärjestelmän välille nämä ratkaisut käyttävät usein huipputeknologioita kuten AI:ta käyttäjän tunnistamisen tarkistamiseen ja arvioimiseen. Iiris- ja äänentunnistusjärjestelmät, sormenjälkitunnistimet kuten

TouchID, ja kasvojentunnistustekniikka ovat yleisiä esimerkkejä. Sisäisten MFA-työkalujen turvallisuus ja yksinkertaisuus ovat niiden tärkeimmät edut. Koska he ovat osa käyttäjää, niitä on lähes vaikea menettää eivätkä useimmat hyökkääjät pysty jäljittelemään biometristen tietojen monimutkaisuutta kuten kasvoja. On myös esteitä, sillä biometristen todentamisjärjestelmien on oltava vahvoja ja kehittyneitä, pystyttävä havaitsemaan pieniä yksityiskohtia väärien vastaavuuksien estämiseksi sekä kestämään biometristen tunnisteiden kuten sormenjälkien tai kasvonpiirteiden, muutoksia tai vaurioita. (What Is MFA? n.d.)

Boonkrong (2021) uskoo biometrisiin tietoihin perustuvan todentamisen tarjoavan enemmän turvallisuutta kuin pelkän salasanan sisältävän järjestelmän. Valitettavasti on myös osoitettu, että biometrisellä todentamisella on haavoittuvuuksia, koska jotkin käyttäytymiseen liittyvät ja fysiologiset biometriset tiedot kuten kirjalliset allekirjoitukset, voidaan väärentää, samoin kuin jotkut fysiologiset biometriset tiedot kuten sormenjäljet. Siksi, jotta voidaan luoda monivaiheinen biometrinen todentaminen, vain biometrisiin todentamismenetelmiin on lisättävä muita todentamistekijöitä. (Boonkrong 2021, 141.)

3.4.4 Uudet todentamistekijät

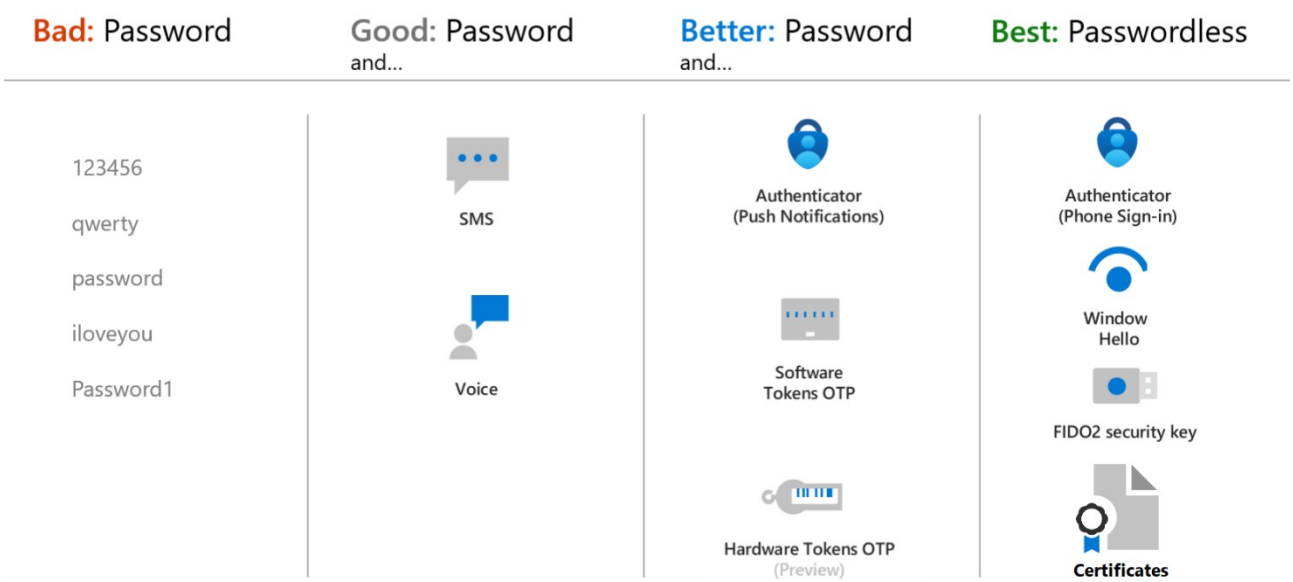
Boonkrong (2021, 139) käsittelee uusien todentamistekijöiden käyttöönottoa monivaiheisessa todentamisessa ja huomauttaa, että turvallisuusasiantuntijoiden on harkittava useampia kuin kahta tekijää. Hän mainitsee, että järjestelmän ja palvelimen aikasynkronointi on tärkeää tarkan monivaiheisen todentamisen kannalta, koska aikatekijä rajoittaa pääsyä riippuen todennäköisyydestä, että käyttäjä kirjautuu sisään ennalta määrättyjen aikojen sisällä. Boonkrong (2021, 139) korostaa sijaintitekijän merkitystä, jossa käyttäjän rekisteröityä sijaintia verrataan nykyiseen kirjautumisyritykseen käyttäen IP- ja GPS-tietoja aitouden tarkistamiseen, mikä lisää maantieteellisen komponentin. Hän mainitsee myös ympäristön äänitekijän, joka parantaa turvallisuutta varmistamalla käyttäjän fyysisen läsnäolon sisäänkirjautumispisteen lähellä, sekä kuulovarmennuksen, joka tunnistaa käyttäjän älypuhelimen erottuvan äänimerkin. Boonkrong (2021, 139) korostaa, että identiteetin vahvistamiseen tarvitaan enemmän elementtejä monivaiheisessa todentamisessa, mikä tekee kulunvalvontajärjestelmät yleisesti turvallisemmiksi. Hän muistuttaa kuitenkin, että käytettävyys ja mukavuus ovat edelleen haasteita, joita on tärkeä ottaa huomioon. Lopuksi hän toteaa, että järjestelmän suojaamiseksi tunkeilijoilta tarvitaan tehokkaampi todentamisprosessi ja

että tulevaisuudessa suunniteltavat monivaiheiset todentamisprotokollat voivat hyödyntää monipuolisesti erilaisia todentamistekijätyyppejä. (Boonkrong 2021, 139.)

Näistä uudemmista todentamistekijöistä käyttäjän maantieteellisen sijainnin hyödyntäminen identiteetin vahvistamiseksi estää usein pääsyn odottamattomilta alueilta kuten silloin, kun suoratoistopalvelu kieltäytyy sallimasta kirjautumisyrityksiä tunnistamattomilta alueilta. Tämä tekniikka varmistaa, että käyttäjä on tunnetussa laitteessa tai luotetussa paikassa käyttämällä aiemmin mainittuja IP-osoitteita tai GPS-signaaleja tietoina. Tämä lähestymistapa on usein edullinen ja vaatii vain vähän käyttäjien työtä, mutta se tarjoaa myös vahvan suojakerroksen, mikä vaikeuttaa hyökkääjien, joilla on salasana ja TOTP luomasta uudelleen käyttäjän ainutlaatuisen sijainnin. Siitä huolimatta on olemassa tietosuojaongelmia, koska jatkuva sijainnin seuranta tai IP-osoitteen jakaminen vaadittaisiin, ja verkko-ongelmat voivat ajoittain estää todentamisen, mikä vaikeuttaa valtuutettujen käyttäjien pääsyä tietyille alueille. (What Is MFA? n.d.)

3.5 Todentamismenetelmät

Todentamistekijät ja todentamismenetelmät ovat läheisesti liittyviä, mutta ne eivät ole täysin sama asia. Kuviossa 4 havainnollistetaan todentamismenetelmien olevan konkreettisia keinoja, joilla todentamistekijät toteutetaan käytännössä. Esimerkiksi salasanan syöttäminen, tekstiviestillä saadun koodin käyttäminen tai biometrisen tunnisteen skannaus ovat kaikki todentamismenetelmiä. Ne ovat tapoja, joilla todentamistekijöitä sovelletaan käyttäjän tunnistamiseksi. Lyhyesti sanottuna, todentamistekijät ovat yleisiä luokkia tai periaatteita, jotka määrittävät, minkä tyyppistä todisteita käyttäjän identiteetistä tarvitaan, kun taas todentamismenetelmät ovat näiden periaatteiden konkreettisia sovelluksia.



Kuvio 4. Todentamismenetelmät Microsoft Entran MFA:ssa (How it works: Microsoft Entra multifactor authentication 2023)

Sham (2021) korostaa todentamismenetelmien tärkeyttä monivaiheisen todentamisen toteuttamisessa. Hänen mukaansa nämä menetelmät mahdollistavat käyttäjien identiteetin varmistamisen käyttämällä useampaa kuin yhtä aiemmin mainittua todentamistekijää. Lisäämällä suojakerroksia, monivaiheiset todentamismenetelmät lisäävät merkittävästi turvallisuutta vaikeuttamalla luvattomien osapuolten pääsyä verkkoihin, järjestelmiin ja sovelluksiin. Sham (2021) mainitsee, että kun sijaintiin perustuvaa todentamista käytetään yhdessä tavanomaisempien MFA-tekijöiden, kuten PIN-koodien tai kertaluonteisten salasanojen kanssa, se hyödyntää laitteen IP-osoitetta ja maantieteellistä sijaintia käyttäjien vahvistusmenettelyjen parantamiseksi. (Sham 2021.)

Sham (2021) kuvaa myös riskiin perustuvaa todentamista, joka tunnetaan adaptiivisena todentamisena, joka dynaamisesti säätää todentamisehtoja. Tämä menetelmä yhdistää vahvan suojauksen ja käyttömukavuuden arvioimalla kontekstia, mukaan lukien laitteet, verkkoasetukset ja käyttäjän tavanomaiset paikat, määrittääkseen tarvittavan oikean todentamisasteen. Hän mainitsee myös salasanattoman todentamisen, joka on entistä progressiivisempi askel luopumalla tavallisesta salasanasta, joka usein aiheuttaa tietoturvaloukkauksia heikkojen ja uudelleenkäytettävien salasanojen vuoksi. Salasanattomassa todentamisessa käytetään korkean varmuuden tekijöitä, ku-

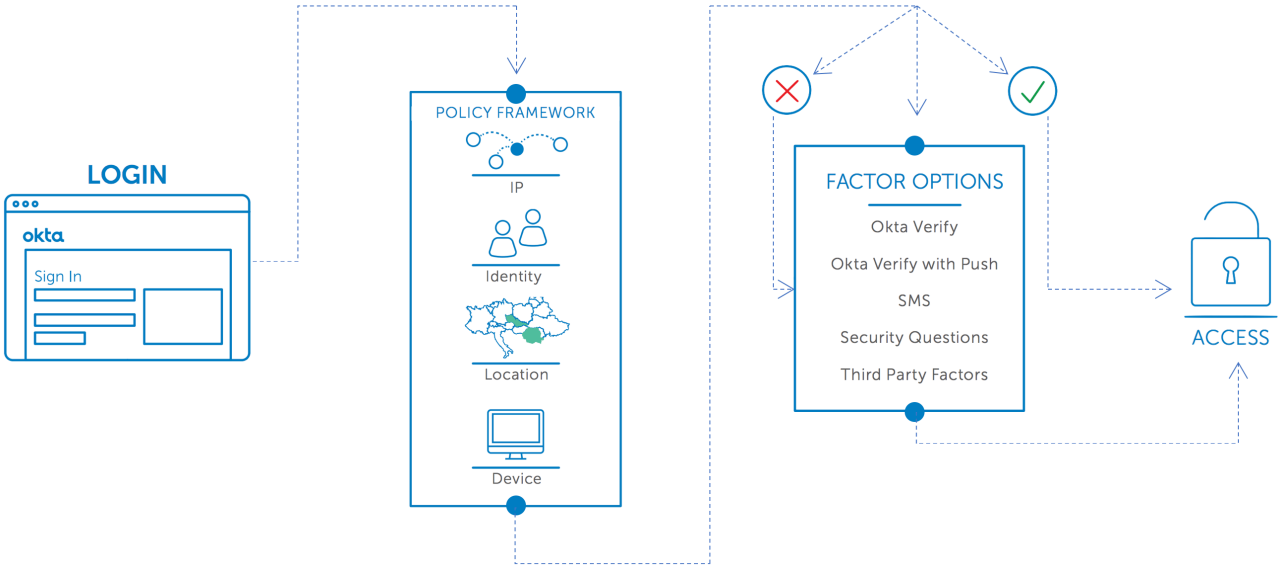
ten FIDO2.0 ja WebAuthn, jotka käytännössä poistavat haavoittuvuudet, jotka liittyvät vaarantuneisiin valtuustietoihin. Se yhdistää tämän kontekstuaalisiin ominaisuuksiin kuten sijaintiin, riskinarviointiin, käyttäytymismalleihin ja laitteen tilaan. (Sham 2021.)

4 Monivaiheisen todentamisen palveluntarjoajat

Tässä kappaleessa tarkastellaan, kuinka monivaiheisen todentamisen palveluntarjoajat ovat keskeisessä roolissa nykypäivän tietoturvastrategioissa. Korostetaan, että nämä palvelut tuovat lisäsuojaa perinteiseen salasanaan verrattuna tarjoamalla useita todentamistasoja. Tämä voi sisältää esimerkiksi token-laitteiden, mobiilisovellusten tai biometristen tunnisteiden käyttöä. Kappaleen keskeinen osa keskittyy markkinoiden johtaviin toimijoihin, kuten Cisco Duo Security MFA, Okta Adaptive MFA, Microsoft Entra MFA, RSA MFA ja LastPass MFA. Nämä palvelut esitellään niiden käytettävyyden, integraatiokyvyn, mukautettavuuden ja hinnoittelun näkökulmasta, mikä tekee niiden vertailusta sekä tärkeää että monimutkaista. Erityisesti Cisco Duon ja muiden palveluntarjoajien vertailu on avainasemassa, sillä se arvioi näiden kykyä vastata liiketoiminnan tarpeisiin, säädösten noudattamiseen ja tietoturvaan. Tämä vertailu on suunnattu auttamaan yrityksiä valitsemaan oikean MFA-ratkaisun, joka yhdistää turvallisuuden, helppokäyttöisyyden ja taloudellisen tehokkuuden vaatimukset. Kappaleen tarkoituksena on siis tarjota kattava ja informatiivinen yleiskatsaus MFA-ratkaisujen nykytilasta ja auttaa lukijaa ymmärtämään, miten nämä ratkaisut voivat tukea heidän tietoturvatarpeitaan.

4.1 Okta Adaptive monivaiheinen todentaminen

Kuviossa 5 havainnollistetaan Okta Adaptive monivaiheinen todentamisen yhdistävän yritystason suojauksen ja sujuvan käyttökokemuksen, paikkaavan vanhentuneiden ja eristäytyneiden MFA-ratkaisujen puutteita. Se merkitsee siirtymistä kohti harkitumpaa, lähestyttävämpää ja kattavampaa turvallisuusparadigmaa. Okta vähentää riskejä hallitsemalla sovellusten ja tietojen käyttöä käyttämällä käytäntöihin perustuvaa kontekstuaalista käyttöoikeuksien hallintaa, joka tutkii käyttäjän kontekstin mukaan lukien sijainnin ja laitteen pääsyn hallintaan. Pääsyä voidaan säätää tarkasti sallimaan tai kieltämään käyttäjän toiminnot hetken kontekstin perusteella. MFA-järjestelmä virtaviivaistaa käyttäjän rutiineja pyytämällä lisätodentamista vain tarvittaessa. (Moving Beyond User Name & Pasword n.d.)



Kuvio 5. Okta Adaptive MFA:n toiminta (Moving Beyond User Name & Pasword n.d)

IT-osastojen ei tarvitse huolehtia laitteistorajoituksista tai ulkomaan pääsyn ongelmista, koska ratkaisu on laajalti yhteensopiva nykyaikaisten todentamistekijöiden kanssa. Okta kattaa suuren määrän käyttäjätilanteita, mikä helpottaa siirtymistä muista järjestelmistä, kuten RSA:sta. Näitä ovat tekstiviestipääsykoodit, kolmannen osapuolen tunnukset, kuten Yubikey, ja älypuhelinpohjainen vahvistus, kuten Okta Verify with Push. Turvallisuuden parantamiseksi ja tukikysymysten vähentämiseksi järjestelmänvalvojat voivat valita, mitkä vahvistusprosessit ovat pakollisia tai tarpeettomia tietyille käyttäjäryhmille. Big datan analytiikan avulla Oktan ennakoiva riskipohjainen metodologia luo kattavia käyttäjäprofiileja tarkkoja riskien arviointeja varten, mikä mahdollistaa mahdollisten riskien varhaisen havaitsemisen. Yhdistämällä tämä hienostunut analytiikka liiketoiminnan liikkuvuuden hallintaan ja Oktan kertakirjautumistietoihin tietoturvakuva on kattavampi ja hyökkääjien on vaikea tunkeutua. Kun epätavallista toimintaa havaitaan, Okta Adaptive MFA tekee muutakin kuin vain ilmoittaa järjestelmänvalvojille, sillä se myös ryhtyy välittömiin toimiin kyseenalaisen toiminnan lopettamiseksi tai rajoittamiseksi, mikä vähentää merkittävästi riskiä. Lisäksi Okta Application Networkissa tarjottavien monien liittimien ansiosta Oktan pilvipohjainen arkkitehtuuri tekee uusien sovellusten ja VPN-verkkojen lisäämisen yksinkertaiseksi säilyttäen samalla yhdenmukaiset sovellus- ja käyttäjäturvastandardit. (Moving Beyond User Name & Pasword n.d.)

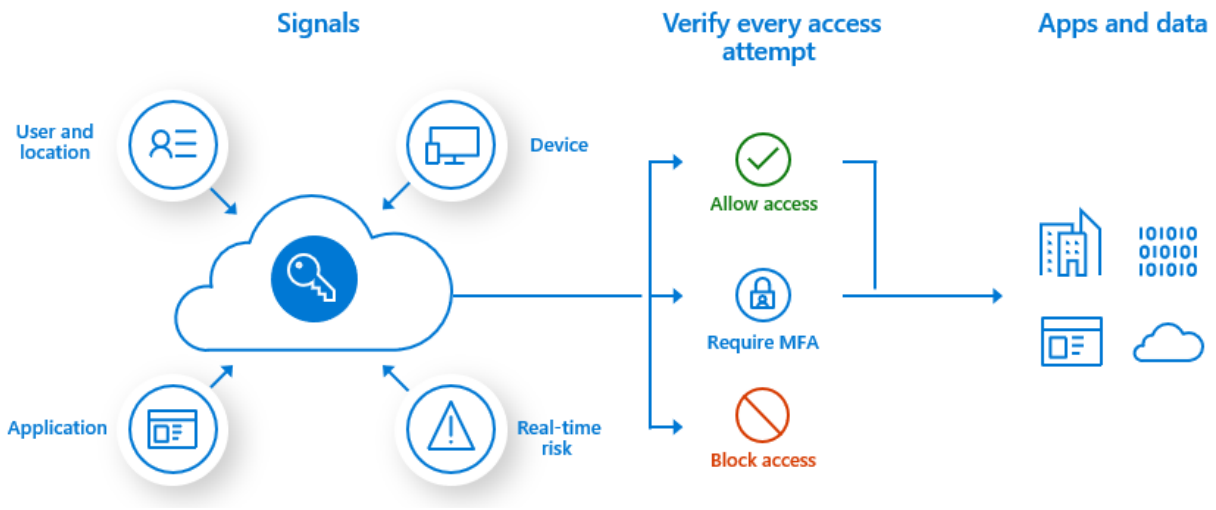
Lisäksi tarjoamalla kehittäjille sovellusliittymiä ja Okta Sign-on -widgetin, Okta Adaptive MFA antaa heille mahdollisuuden sisällyttää vaivattomasti vahvan todentamisen ainutlaatuisiin sovelluksiin,

mikä mahdollistaa täysin tuotemerkityn MFA-kokemuksen, joka täydentää organisaation suunnittelua. Pohjimmiltaan Okta Adaptive MFA tarjoaa IT- ja tietoturva-ammattilaisille ratkaisun, joka suojaa sovelluksia ja infrastruktuuria ja tarjoaa samalla saumattoman, mukautuvan käyttökokemuksen kaikki edullisen, skaalautuvan pilvipohjaisen arkkitehtuurin sisällä. (Moving Beyond User Name & Pasword n.d.)

4.2 Microsoft Entra monivaiheinen todentaminen

Kun käyttäjät muodostavat yhteyden sovellukseen tai palveluun ja he saavat monivaiheisen todentamisen kehotteen, heille näytetään luettelo lisävahvistusvaihtoehdoista, jotka he ovat jo määrittäneet profiiliinsa. Näitä valintoja voidaan hallita, joko lisätä tai muuttaa käyttämällä "Oma profiili" -toimintoa. Tarjoamalla laajan valikoiman ylimääräisiä varmennustekniikoita Microsoft Entra ID parantaa käyttäjätilien turvallisuutta. Nämä koostuvat monipuolisesta Microsoft Authenticator -ohjelmistosta, Outlookiin integroidusta Authenticator Liten optimoidusta versiosta ja huippuluokan Windows Hello for Businessista, joka yksinkertaistaa pääsyä biometristen koodien avulla. FIDO2-suojausavain on luotettava valinta henkilöille, jotka pitävät fyysisistä turvalaitteista. Käyttäjät voivat myös valita aikapohjaisia koodeja luovan OATH-ohjelmistotokenin tai ja sen laitteistotokenin, joka on nyt esikatselussa. Myös perinteiset tekniikat otetaan huomioon; puhelu- ja tekstiviestivahvistukset ovat edelleen luotettava osa monivaiheista suojausstrategiaa, jota Microsoft Entra ID:n monivaiheinen todentamisen järjestelmä kannattaa. (How it works: Microsoft Entra multifactor authentication 2023.)

Kuviossa 6 on kuvattu pääpiirteittäin Microsoft Entran monivaiheinen todentamisen toiminta, joka voidaan ottaa käyttöön käyttämällä vähintään kahta todentamistekijää ja niihin liittyviä menetelmiä: jotain mitä tiedät, jotain mitä omistat ja biometriset tiedot. Salasanan nollausturvaa voidaan parantaa käyttämällä Microsoft Entran monivaiheista todentamista. Käyttäjät voivat rekisteröityä yksivaiheiseen itsepalvelusalasanan vaihtoon rekisteröityessään Microsoft Entran monivaiheista todentamista varten. Määritysvalintojen perusteella järjestelmänvalvojat voivat asettaa MFA-haasteita ja valita lisätodentamismenetelmiä. Microsoft Entran monivaiheisen todentamisen hyödyntäminen ei edellytä sovellusten ja palveluiden päivittämistä. Microsoft Entran kirjautumismenettely, joka kysyy ja käsittelee automaattisesti MFA-haasteen tarvittaessa sisältää myös varmistuskysymykset. (How it works: Microsoft Entra multifactor authentication 2023.)



Kuvio 6. Microsoft Entra MFA:n toiminta (Microsoft 2023)

Microsoft Entra vuokralaisilla on mahdollisuus ottaa Microsoft Authenticator välittömästi käyttöön kaikille käyttäjille käyttämällä suojausoletusasetuksia. Microsoft Entran monivaiheista todentamista voidaan käyttää ylimääräisen vahvistuksen vaatimiseen henkilöiden ja ryhmien kirjautumisen aikana. Ehdollisia käyttösääntöjä voidaan käyttää määrittämään tapahtumia tai ohjelmia, jotka tarvitsevat monivaiheista todentamista tarkempaan hallintaan. Kun käyttäjä on yrityksen verkossa tai rekisteröidyssä laitteessa, nämä säännöt voivat sallia rutiinikirjautumisen; mutta jos käyttäjä on etäällä tai käyttää henkilökohtaista laitetta, hän saattaa tarvita ylimääräisiä vahvistustietoja. (How it works: Microsoft Entra multifactor authentication 2023.)

4.3 RSA monivaiheinen todentaminen

Kuviossa 7 on näytetty maailman laajimmin käytetyn RSA:n monivaiheisen todentamisen vaiheet ja se on osoitus sen laajasta hyväksynnästä ja joustavasta käytöstä. Sen suosio johtuu vahvojen turvaominaisuuksien ja käyttäjäystävällisten ominaisuuksien yhdistelmästä, jotka on suunniteltu tyydyttämään sekä ihmisten että yritysten erilaiset tarpeet. Käyttäjät voivat valita laajasta valikoimasta todentajia, jotka vastaavat erilaisia vaatimuksia ja vaihtelevat push-to-prove-tekniikoiden ja kertakäyttöisten salasanojen joustavuudesta helppokäyttöisyyteen ja biometristen tietojen, kuten sormenjälkien ja kasvojentunnistuksen korkeaan turvallisuuteen. Lisäksi RSA tarjoaa tavanomaisia laitteistotokeneita, edistää henkilökohtaisten todentajien käyttöä ja mahdollistaa FIDO-pohjaisen todentamisen. (Multi-Factor Authentication 2022.)

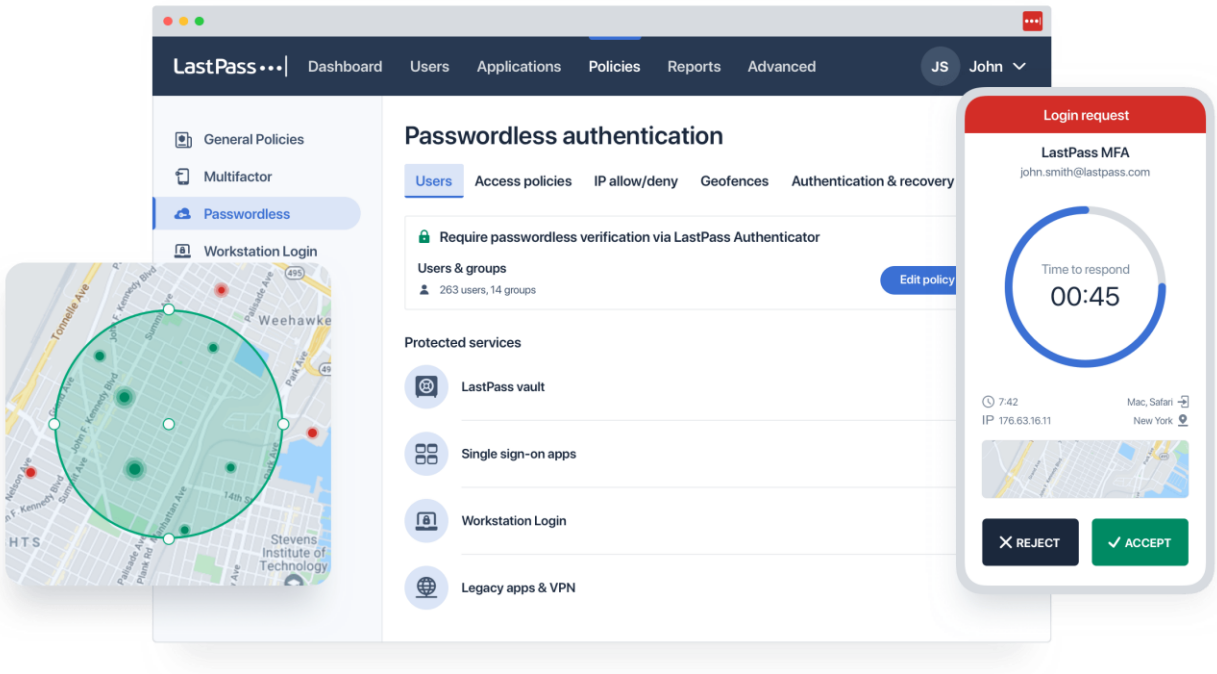
Kuvio 7. RSA MFA:n vaiheet (What is Multi-Factor Authentication (MFA) and How does it Work? 2021)

Tämä sopeutumiskyky yhdistyy taktiseen etuun, jonka avulla on mahdollista yhdistää pilvipalvelut paikan päällä oleviin todentamisjärjestelmiin sujuvasti ja asteittain, jotta organisaation sisällä voidaan mukauttaa räätälöityjä pilvipalvelustrategioita. RSA osoittaa sitoutumisensa saatavuuteen ja luotettavuuteen 99,95 % käyttöaikatakuulla ja erityisellä ei epäonnistunut -ominaisuudella, joka pitää turvallisen ja jatkuvan käytön Windowsissa ja macOS:ssa jopa verkkokatkosten sattuessa. (Multi-Factor Authentication 2022.)

RSA:n monivaiheisen todentamisen ratkaisun soveltamisalaan kuuluvat RSA Ready -teknologiaintegraatiot, joista jokainen on testattu ja dokumentoitu kattavasti varmennettujen yhteensopivuuden takaamiseksi useissa käyttötilanteissa. Tämä strategia ei ainoastaan osoita, kuinka sitoutunut RSA on ylläpitämään korkeita turvallisuusstandardeja, vaan se luo myös ilmapiirin, joka on valmis lisäämään integraatioita avoimien standardien kautta tulevaisuudessa. RSA:n ratkaisut tarjoavat houkuttelevan vaihtoehdon yrityksille, jotka haluavat parantaa tietoturva-asentoaan monivaiheisen todentamisen avulla riippumatta siitä toimivatko ne pilvessä vai paikan päällä. Tämä johtuu siitä, että RSA:n ratkaisut turvaavat pääsyn ja säilyttävät samalla käyttäjäystävällisyyden. (Multi-Factor Authentication 2022.)

4.4 LastPass monivaiheinen todentaminen

LastPassin monivaiheinen todentaminen virtaviivaistaa työntekijöiden kirjautumisprosesseja ja suojaa samalla yritystä turvallisella biometrisellä todentamisella. LastPass MFA takaa verkossa ja vanhoissa sovelluksissa, VPN:ssa ja työasemissa, että oikeat ihmiset käyttävät oikeita tietoja oikeaan aikaan ilman, että se lisää monimutkaisuutta. Se käyttää kuviossa 8 näkyvää erityistä tietoturva-lähestymistapaa, joka takaa biometristen tietojen yksityisyyden ja turvallisuuden samalla, kun se käyttää kontekstuaalisia ja biometrisiä muuttujia käyttäjien tunnistamiseen ja todentamiseen, vaikka he eivät olisi verkossa. LastPass tarjoaa samassa salasanattoman monivaiheisen todentamisen kokemuksen, joka on järjestelmänvalvojien helppo ottaa käyttöön ja henkilöstön jäsenten käyttää. (LastPass MFA offers a passwordless experience for users 2019.)



Kuvio 8. LastPass MFA:n esittely (MULTIFACTOR AUTHENTICATION INTEGRATIONS n.d)

LastPass MFA tarjoaa myös mukautuvan todentamisjärjestelmän, joka integroituu sujuvasti käyttäjien tarpeisiin hyödyntämällä biometrisiä tekijöitä, kuten sormenjälkiä ja kasvojentunnistusta sekä kontekstuaalista älykkyyttä, kuten laitteen sijaintia ja IP-osoitetta henkilöllisyyden vahvistamiseksi vaivattomasti ja ilman ylimääräistä vaivaa kirjautumisen aikana. Tämä menetelmä tarjoaa salasanattoman kokemuksen, joka ei vain vähennä turhautumista vaan myös vähentää tietoturvariskejä.

Ratkaisu on suunniteltu helppoa käyttöönottoa varten eikä se vaadi IT-tiimien lisäkoulutusta, ja siinä on vaiheittaiset ohjeet sujuvan käyttöönoton varmistamiseksi. Se lupaa kitkattoman käyttökokemuksen turvaamalla jokaisen tukiaseman ja helpottamalla saumatonta todentamista eri laitteissa, mikä parantaa tuottavuutta turvallisuudesta tinkimättä. LastPass MFA tarjoaa keskitetyn, yksityiskohtaisen hallinnan, jonka avulla yritykset voivat valvoa tiettyjä pääsykäytäntöjä, joita hallitaan yhdistetystä järjestelmänvalvojan hallintapaneelista. Järjestelmä on suunniteltu plug-and-play -integraatioilla, mikä mahdollistaa automaattisen käyttäjien provisioinnin hakemistoissa, kuten AD, Microsoft Entra ID, Okta ja OneLogin, ja se skaalautuu vaivattomasti yrityksen kanssa. LastPass MFA on all-in-one-todentamisratkaisu, joka tukee pilvi-, mobiili-, vanhoja, paikallisia sovelluksia, VPN-verkkoja ja työasemia ja virtaviivaistaa todentamisen hallintaa yksittäisestä käyttöliittymästä. Turvallisuutta priorisoiva LastPass MFA varmistaa, että biometriset tiedot pysyvät yksityisinä ja suojattuina, salataan käyttäjän laitteessa ja eivät koskaan keskitetä, mikä suojaa palvelinpuolen tietomurroilta. (LastPass MFA offers a passwordless experience for users 2019.)

5 Cisco Duo

Tässä kappaleessa esitellään Cisco Duon rooli monitasoisena tietoturva-alustana, joka on räätälöity tukemaan organisaatioita niiden pyrkimyksissä suojata identiteettejä ja tietoja. Alustan useat identiteetin vahvistus- ja turvallisuusominaisuudet tuodaan esille, korostaen sen erityistä suunnittelua digitaalisten resurssien suojaamiseen monimutkaisessa uhkaympäristössä. Kappaleessa käsitellään myös, kuinka Frendy on ottanut tietoturvan vakavasti ja valinnut Cisco Duon monivaiheisen todentamisen ratkaisuksi. Tämä valinta korostaa Cisco Duon kykyä tarjota vahva ja monipuolinen suojaus tietoja ja järjestelmiä vastaan.

Erityisen huomion kohteena on, miten Cisco Duo muuttuu monivaiheiseksi todentamiseksi Trusted Endpoints -käytännön käyttöönoton myötä. Tässä yhteydessä korostetaan, kuinka päätepisteen on täytettävä Duo Desktopin asettamat vaatimukset kirjautumisen onnistumiseksi. Tämä osa kappaleesta valottaa konkreettisesti, miten Cisco Duon käyttöönotto voi parantaa organisaation tietoturvan tasoa. Kappaleen tavoitteena on tarjota lukijalle selkeä kuvaus Cisco Duon monivaiheisen todentamisen hyödyistä ja sen roolista Frendyn tietoturvastrategiassa.

Cisco Duon monivaiheisessa todentamisessa käytetään useita todentamiselementtejä, jotka tarjoavat vahvan suojauksen, joka on mukautuva käyttäjille ja silti joustamaton hyökkäyksiä vastaan.

Käyttöliittymän avulla käyttäjät voivat tunnistautua helposti, nopeasti ja vaivattomasti, jolloin he voivat keskittyä todella tärkeisiin asioihin. Duon suuren skaalautuvuuden ja helpon integroinnin ansiosta useimpiin suosittuihin sovelluksiin sekä räätälöityihin sovelluksiin on mahdollista ottaa käyttöön turvallinen pääsyratkaisu ilman IT:n apua. Useita vahvoja todentamistekniikoita, kuten pääsykoodit, tunnukset, biometriset tiedot, Duo Push -mobiilisovellus ja paljon muuta on saatavana monivaiheisen todentamisen kanssa. Käyttäjät voivat ottaa monivaiheisen todentamisen käyttöön nopeasti ja helposti Duon monivaiheisen todentamisen -mobiilisovelluksen Duo Mobile avulla. Kyseinen sovellus yksinkertaistaa kirjautumisprosessia ja helpottaa vahvistamista mobiililaitteilla. Tämä alentaa kokonaiskustannuksia ja helpottaa samalla asiakkaiden monivaiheisen todentamisen käyttöönottoa. (Multi-Factor Authentication (MFA) n.d.)

Cisco Duon kaksivaiheinen todentaminen vaatii kahta eri tapaa varmistaa käyttäjän identiteetti ja vahvistaa huomattavasti sovellusten ja ympäristön turvallisuutta lisäämällä luottamusta siihen, että käyttäjät ovat niitä, joita he sanovat olevansa. Tällainen monivaiheinen todentaminen tarjoaa vahvan suojan tietojenkalastelua, sosiaalista manipulointia ja salasanojen raa'an voiman hyökkäyksiä vastaan yhdistämällä käyttäjän tiedot, kuten hänen kirjautumistunnuksensa ja salasanansa, omaisuuteensa kuten älypuhelinsovelluksen valtuuttamat todentamispyynnöt. 2FA on olennainen osa nollaluottamusta suojaavaa arkkitehtuuria. Se suojaa arkaluontoisia tietoja todentamalla käyttäjiä ja estämällä useita tietoturvahyökkäyksiä, joiden tarkoituksena on vaarantaa käyttäjien salasanat ja tilit. Kun jokaiselle todentamiselementille, kuten mobiiliverkkoon, käytetään erillisiä kanavia push-ilmoitusten hyväksyntää varten, tämä lähestymistapa estää erittäin menestyksekkäästi kaukaisia hyökkääjiä saamasta luvatonta pääsyä jopa siinä tapauksessa, että he onnistuvat tunkeutumaan pääverkkoon. Kaksivaiheista todentamista käyttävät sovellukset varmistavat, että hakkerit eivät voi käyttää tilejä ilman todentamiselementtiin tarvittavaa fyysistä laitetta. Duolla käyttäjien tarvitsee vain kantaa älypuhelinta Duo Mobile -sovelluksen ollessa asennettuna, mikä tekee 2FA:sta yksinkertaisen ja helpon käyttää. Duo tarjoaa turvallisen ja käytännöllisen vastauksen nykyaikaisiin todentamisongelmiin, koska se tukee laajaa valikoimaa todentamistekniikoita ja sen joustavuus vastaa erilaisten käyttäjien vaatimuksiin. (Two-Factor Authentication (2FA) n.d.)

5.1 Edut

Tässä kappaleessa keskitytään Cisco Duon tarjoamiin ominaisuuksiin, jotka erottavat sen kilpailijoista tehokkaana, mutta samalla käyttäjäystävällisenä tietoturvaratkaisuna. Tarkastellaan, kuinka

Cisco Duon monivaiheisen todentamisen implementointi voi tukea organisaatioita heidän pyrkimyksissään vahvistaa tietoturvaa, parantaa käyttäjien kokemusta ja kohdata nykyaikaisen digitaalisen maailman asettamat haasteet. Seuraavissa luvuissa syvennytään näihin merkittäviin ominaisuuksiin, tarjoten yksityiskohtaista tietoa niiden toiminnallisuudesta ja hyödyistä. Tämä lähestymistapa antaa lukijalle perusteellisen käsityksen Cisco Duon roolista tietoturvan alalla ja sen merkityksestä nykyaikaisten organisaatioiden tietoturvastrategioissa.

5.1.1 Helppous ja yksinkertaisuus

Kyberturvallisuuden monimutkaisuuden tavoitteena on kävellä hyökkääjien sekä kuluttajien varpailla. Cisco Duon ratkaisu, joka on yksinkertaisin MFA-järjestelmä sekä käyttäjille että järjestelmänvalvojille, perustuu tähän filosofiaan. Verified Duo Push ja Duo Mobile, jotka ovat erinomaisia esimerkkejä omistautumisesta yksinkertaiseen ja helppokäyttöiseen todentamisprosessiin. Käyttäjät voivat muuttaa matkapuhelimensa tehokkaiksi tietoturvatyökaluiksi muutamalla kosketuksella. Se on yhtä helppoa kuin Duo Push -sovelluksen lataaminen. Turvalliseen pääsyyn on vain yksinkertainen reitti eikä ole monimutkaisia asetuksia tai työläitä tehtäviä. Tämä käytön yksinkertaisuus on esimerkki siitä, että vahvan tietoturvan pitäisi antaa käyttäjille enemmän valtaa kuin rasittaa heitä rakentamalla linnoitus, joka ärsyttää tunkeilijoita ja toivottaa valtuutetut käyttäjät lämpimästi tervetulleeksi. (Multi-Factor Authentication (MFA) n.d.)

5.1.2 Mukautuva todentaminen

Käyttäen Duon mukautuvaa todentamista, joka edustaa monivaiheisen todentamisen uusinta kehitystä, voit turvallisesti vastata nykypäivän yritysten jatkuvasti muuttuviin vaatimuksiin. Tämä ratkaisu on suunniteltu tarjoamaan sekä turvallisuutta että joustavuutta. Tämän progressiivisen suojausominaisuuden avulla on mahdollista luoda mukautettuja pääsynhallintalaitteita, jotka mukautuvat automaattisesti monenlaisiin kontekstuaalisiin olosuhteisiin. Duon mukautuva todentaminen varmistaa, että tietoturva on yhtä mukautuva kuin se on vahva riippumatta siitä määräytyvätkö käyttöoikeudet käyttäjän roolin, käytettävän sovelluksen herkkyyden, sisäänkirjautumisyrityksen sijainnin, verkon suojauksen eheyden tai liitäntälaitteen kunnon mukaan. Suojauskerroksia ei pitäisi vain lisätä vaan niiden tulee myös olla älykkäitä ja reagoivia, jotta ne suojaavat digitaalista omaisuuttasi ja tarjoavat saumattoman sekä käyttäjäystävällisen käyttökokemuksen. (Multi-Factor Authentication (MFA) n.d.)

5.1.3 Salasanattomuus

Duo Passwordless Authentication, joka on innovatiivinen lisä perinteiseen monivaiheiseen todentamiseen, tarjoaa vankan pohjan salasanattomalle tulevaisuudelle edistäen nykyaikaista turvallisuuskäytäntöä. Tämän järjestelmän perustana on käyttäjän henkilöllisyyden vahvistusprosessi, jossa käytetään huippuluokan kirjautumistyökaluja, kuten biometrisiä tietoja, suojausavaimia ja käyttäjäystävällistä Duo Push -mobiilisovellusta. Duon salasanattoman todentamisen viehätys piilee sen yksinkertaisuudessa ja käyttäjälähtöisessä suunnittelussa. Käyttäjät voivat nauttia vaivattomasta ja sujuvasta pääsystä ilman tarvetta syöttää monimutkaisia salasanoja. Tämä tapahtuu sen jälkeen, kun he ovat kerran vahvistaneet henkilöllisyytensä määritellyn aikarajan sisällä, jonka järjestelmänvalvojat ovat asettaneet. Tämä yksinkertaistettu, yksivaiheinen vahvistustapa mullistaa kirjautumisprosessin ja tekee siitä yksinkertaisempaa ja turvallisempaa. Duon avulla turvallinen pääsy muuttuu erilliseksi vahvaksi portinvartijaksi, jonka avulla käyttäjät voivat olla vuorovaikutuksessa digitaalisen työtilansa kanssa ennennäkemättömällä yksinkertaisella tavalla. (Multi-Factor Authentication (MFA) n.d.)

5.1.4 Skaalautuvuus

Duon monivaiheisen todentamisen ratkaisu kasvaa yrityksesi mukana toimien mukautuvana yhdyskäytävänä, joka liittää saumattomasti sekä nykyisen että tulevan IT-infrastruktuuriin. Koosta riippumatta se on täydellinen suoja kasvaville yrityksille, koska sen avulla on helppoa integroida uusia ihmisiä ja laitteita. Duon rakenne on rakennettu ketteryyttä ajatellen, mikä mahdollistaa uusien sovellusten suojaamisen lähes reaaliajassa ja varmistaa samalla, että olemassa olevat järjestelmäsi ovat turvallisia. Sujuvan skaalautuvuuden ansiosta tietoturvatoimenpiteet laajenevat yrityksen kasvun mukana ilman, että ne monimutkaistuvat tai heikentävät päivittäistä toimintaa ohjaavan teknologian toimivuutta. Tietoturvasi skaalaaminen Duolla on yksinkertainen toimenpide, joka pysyy yrityksesi tavoitteiden kasvun ja nopeuden mukana. (Multi-Factor Authentication (MFA) n.d.)

5.1.5 Nopea käyttöönotto

Monivaiheisen todentamisen asennuksen ei tarvitse olla työläs tai hidas prosessi. Cisco Duo tarjoaa erittäin yksinkertaisen tavan parantaa tietoturvatasoa. Koska se on yhteensopiva minkä tahansa nykyisen alustan tai ympäristön kanssa, se välttää tyypilliset tekniset ongelmat ja tarjoaa

saumattoman integraatiokokemuksen. Duon itserekisteröitymistoiminto, jonka ansiosta käyttäjät voivat määrittää itsensä ilman vaativaa IT-tukea on pelinmuuttaja. Sen käyttäjälähtöinen suunnittelu todella loistaa tässä yhteydessä, tarjoten vaivattoman ja tehokkaan kokemuksen. Tämä yksinkertaistettu konfigurointi nopeuttaa käyttöönottoa yrityksessä ja vähentää samalla IT-henkilöstön rasitusta. Pitkälle kehitetyn tietoturvan vaikeiden toteutusten päivät ovat takana Duon nopean ja helpon käyttöönoton ansiosta. Nyt tehokas monivaiheinen todentaminen on helposti saatavilla oleva kyberpuolustussuunnitelmasi kulmakivi. (Multi-Factor Authentication (MFA) n.d.)

5.1.6 Integraatiot

Tietoturvan laajentaminen on helppoa käyttäessä Cisco Duoa. Riippumatta siitä, olivatko tietoturvatarpeesi täydellisestä nollaluottamuskehyksen arkkitehtuurista yhteensopivuuden kannalta ratkaisevaan kaksivaiheiseen todentamiseen, Duo mukautuu helposti vahvan natiivi integraation ansiosta useiden sovellusten ja alustojen kanssa. Sen monipuolisuus ja ennakointi nopeasti muuttuvassa digitaalisessa ekosysteemissä on osoitus sen yhteistoimivuudesta monipilvi-, hybridi- ja paikallisten asetusten välillä. Perinteisten lisäksi Duon puolustuskyvyt kattavat laajan valikoiman työkaluja, kuten SaaS-sovelluksia, kriittistä infrastruktuuria, räätälöityjä sovelluksia ja jopa SSH-käytön vivahteita. Lisäksi Duo ylläpitää suojausta offline-laitteille, BYOD-olosuhteille, VPN-asiakkaille ja etätukipisteille tarjoten kattavan ja luotettavan turvaverkon. Tämän takia Duosta tulee enemmän kuin pelkkä tietoturvatyökalu työkalupakissasi, sillä pikemminkin siitä tulee kulmakivi, joka vahvistaa ja tukee yrityksesi turvatoimia kokonaisvaltaisesti ja progressiivisesti. (Multi-Factor Authentication (MFA) n.d.)

5.2 Todentamismahdollisuudet

Tässä opinnäytetyön osassa keskitytään Cisco Duon tarjoamiin monipuolisiin todentamismenetelmiin, jotka ovat elintärkeitä, kun käyttäjät hakevat pääsyä organisaation järjestelmiin ja resursseihin. Monipuolisuus on avainasemassa, sillä se mahdollistaa organisaatioille räätälöidä todentamisvaihtoehtoja vastaamaan erilaisia käyttäjäprofiileja ja turvallisuusvaatimuksia. Esimerkiksi mobiilisovellus vastaa liikkuvien työntekijöiden tarpeisiin, kun taas tekstiviesti- tai puhelutodentaminen palvelee niitä, joilla ei ole pääsyä älypuhelimeen. Tämä analyysi valottaa, miten Cisco Duon joustavuus ja käyttäjälähtöisyys monivaiheisessa todentamisessa tekevät siitä tehokkaan turvallisuusratkaisun, mikä on merkittävää opinnäytetyön tutkimuskysymyksen kannalta.

Cisco Duon mobiilisovellus Duo Mobile on yleinen vaihtoehto. Käyttäjät voivat ladata sovelluksen älypuhelimeensa tai tablettiinsa. Sovellus tuottaa dynaamisen kertakäyttöisen koodin aina, kun käyttäjä yrittää kirjautua sisään. Tämä koodi on voimassa vain lyhyen ajan ja on voimassa vain yhdellä kerralla, mikä tekee siitä erittäin turvallisen vaihtoehdon. Käyttäjille voidaan lähettää tekstiviestillä kertakäyttöinen koodi, joka on syötettävä kirjautumisen yhteydessä. Tämä on yksinkertainen ja laajasti käytetty menetelmä, joka ei vaadi erillistä sovellusta. Käyttäjille voidaan myös soittaa ja pyytää heitä vahvistamaan identiteettinsä puhelinkeskustelun avulla. Käyttäjät voivat vastata puhelimeen ja vahvistaa pääsyn. Joissakin tapauksissa organisaatiot saattavat käyttää fyysisiä hardware-tokeneita, jotka tuottavat kertakäyttöisiä koodeja. Käyttäjät tarvitsevat tokenin fyysisesti mukanaan päästäkseen järjestelmiin. (Authentication Methods: First Line of Defense n.d.)

5.2.1 Duo Push

Nykyaikaisen kyberturvallisuuden kärjessä on Duo Mobile -sovellus, joka tarjoaa luotettavan ja helppokäyttöisen 2FA-palvelun. Toimittamalla push-ilmoitukset kaksivaiheista todentamista varten suoraan käyttäjien älypuhelimiin se parantaa käyttäjien turvallisuutta takaamalla nopean ja turvallisen kirjautumisen useisiin verkkoihin ja sovelluksiin. Tunnistuksen vahvistaminen on yhtä helppoa kuin ilmoituksen vastaanottaminen, kun käyttäjä on syöttänyt käyttäjätunnuksensa ja salasanansa. Heidän älypuhelimensa Hyväksy-painiketta tarvitsee napauttaa vain kerran, jotta he saavat turvallisen pääsyn lähes välittömästi. Duon älykäs integrointi Apple Watchin kaltaisten laitteiden kanssa tekee siitä helpon käyttää useissa laitteissa, mikä osoittaa sen omistautumisen saumattomalle käyttökokemukselle. New York Timesin Wirecutter valitsi Duon parhaaksi kaksivaiheisen todentamisen sovellukseksi korostaen sen tehokkuutta ja käyttäjäystävällistä suunnittelua. Tämä tunnustus vahvistaa Duon aseman johtavana online-tilien suojaustyökaluna. Wirecutterin tunnustus Duo Mobilesta korostaa sen asemaa erittäin arvostettuna tietoturvaratkaisuna. (One-Tap Authentication With Duo Push n.d.)

Integroimalla Duo Pushiin ylimääräisen suojaustason tämän vahvistuskooditoiminnon kautta, voidaan tehokkaasti vähentää häirintä- ja väsymyshyökkäysten riskejä. Tämä ominaisuus estää onnistuneesti tahattomat hyväksynnät vaatimalla käyttäjiä syöttämään tietyn vahvistusnumeron Duo Push -todentamista tehdessään. Lisäksi se tehostaa petostentorjuntaa ohjaamalla käyttäjät Duo Mobile -sovelluksen petosraporttiominaisuuteen aina, kun luvaton kirjautumisyritys tulee näkyviin. Jos push-ilmoitus on käytössä käytäntöasetuksissa, käyttäjiä pyydetään antamaan kuusi- tai

kolminumeroinen numero Duon yleiskehotteen kirjautumisprosessin aikana. Varmistaaksesi Duo Push -pyynnön ja taataksesi turvallisen kirjautumisen, on tärkeää syöttää tämä koodi huolellisesti käyttäjän todentamislaitteeseen. Tämä välttää tahattomat hyväksynnät, kun käyttäjä ei aktiivisesti pyydä pääsyä sovellukseen. (Duo Administration – Policy & Control 2023.)

5.2.2 WebAuth ja biometriikkatodentaminen

Biometriset anturit ja suojausavaimet voivat korvata tavanomaiset pääsykoodit WebAuthin ansiosta, joka on pelinmuuttaja online-tietoturvatilassa. W3C ja FIDO Alliance työskentelivät yhdessä luodakseen tämän huipputeknologian, joka avaa oven yksinkertaiseen ja turvalliseen käyttäjien todentamiseen. WebAuth hyödyntää kannettavien tietokoneiden ja älypuhelimien sisäänrakennettuja toimintoja voidakseen olla vaivattomasti vuorovaikutuksessa sisäänrakennettujen todentajien, kuten macOS TouchID:n, kanssa, jolloin käyttäjät voivat käyttää tilejään vain yhdellä sormenjäljellä. Tämä hienostunut todentamistekniikka tarjoaa vahvan suojakerroksen etähyökkäystä vastaan, yksilöllisten biometristen tietojen käyttömukavuuden lisäksi ja takaa käyttäjän fyysisen läsnäolon koko todentamisprosessin ajan. Lisäksi WebAuth kannattaa tulevaisuutta, jossa turvallisuutta parannetaan samalla kun se on käyttäjäystävällinen. Muuttaakseen kaikki laitteet turvalliseksi ympäristöksi, tarvitaan yhteistyössä toimiva käyttöjärjestelmä ja verkkoselain. USB-pohjaiset FIDO-suojausavaimet, kuten YubiKey auttavat tilanteessa, jolloin laitteessa ei ole biometristä anturia. Ne tarjoavat yhtä turvallisen kaksivaiheisen todentamiskokemuksen ja suojaavat käyttäjiä tietojenkalastelulta ja muilta vaarallisilta hyökkäyksiltä. (WebAuthn: Biometrics and Security Keys n.d.)

5.2.3 Pääsykoodit ja tokenit

Lukuisten pääsykoodimahdollisuuksien, laitteiston suojaustunnusten ja laajan kolmannen osapuolen laiteyhteensopivuuden ansiosta Duon kaksivaiheinen todentaminen sulautuu helposti jokapäiväiseen toimintaan tehden siitä joustavan tietoturvaratkaisun. Luomalla erityisen pääsykoodin pääsyä varten turvatunnukset, jotka voivat olla USB, älykortti tai Bluetooth-avaimenperä ja ne antavat käyttäjille mahdollisuuden vahvistaa online-identiteettinsä turvallisesti. Duon joustavuus jatkuu monivaiheisessa todentamisessa, jossa kovat tunnukset tarjoavat konkreettisen korvikkeen ja pehmeät tunnukset, kuten Duo Push luovat aikapohjaisia kertakäyttöisiä tunnuskoodeja mobiililaitteissa. Duon tekstiviestipääsykoodit ja puhelimen takaisinsoitto-ominaisuudet varmistavat, että

suojattu todentaminen on ihmisten saatavilla ilman älylaitteita tai internetyhteyttä. Duon ohituskoodit tarjoavat kätevän varmuuskopion epätavallisissa tilanteissa, kuten tilapäinen pääsy tai kun pääpisteet eivät ole käytettävissä. Duon kyky ottaa käyttöön sekä sen omat laitteistotunnisteet, kuten kestävä Duo D-100 että ulkoiset tunnukset, kuten YubiKeys korostaa sen sitoutumista turvalliseen ja intuitiiviseen todentamisprosessiin. (WebAuthn: Biometrics and Security Keys n.d.)

5.3 Sovellusten suojaaminen

Cisco Duon monivaiheisen todentamisen ratkaisu, joka integroituu saumattomasti lukuisiin alustoihin ja palveluihin, kuten paikallisiin verkkoihin, VPN-yhteyksiin, sisällönhallintajärjestelmiin, sähköpostijärjestelmiin ja laitteisiin tehostaa turvallisuutta merkittävästi. Sen avulla on mahdollista suojata monipuolisesti useita sovelluksia yksittäisen ratkaisun kautta. Duon hallintapaneelin kautta asiakkaat voivat lisätä muita sovelluksia Duo-tilin luomisen jälkeen ja valita kullekin palvelulle sopivan suojausvaihtoehdon. Tämä järjestelmä vaatii erityisiä asetuksia erilaisille palvelutyypeille, kuten verkkosovelluksille, Microsoft-palveluille, Unix-järjestelmille ja erilaisille VPN-verkoille. Näille tunnistetiedoille vaaditaan tiukkoja turvatoimia, koska tärkeät komponentit, kuten integrointiavain, salainen avain ja API-isäntänimi ovat välttämättömiä minkä tahansa Duon sovelluksen yksilöimiseksi. Integroinnin jälkeen laite tai järjestelmä on määritettävä Duon yhteensopivuutta varten ja käyttäjät on rekisteröitävä. Erityistä huomiota tulee kiinnittää yhteysvaatimuksiin ja Duon suojausprotokolliin, jotka sisältävät viestinnän SSL/TCP portin 443 kautta ja TLS-standardit. (Duo Administration - Protecting Applications 2023.)

5.3.1 Microsoft Entran ehdollinen pääsy

Cisco Duo pystyy liittymään Microsoft Entra ID:n kanssa parantaakseen Entra ID -kirjautumisia kaksivaiheisen todentamisen avulla. Se tarjoaa itsepalvelulaitteiden hallinnan, sisäänrakennetun käyttäjien rekisteröinnin ja tuen useille todentamismenetelmille mukaan lukien salasanat, suojausavaimet, Duo Push ja Verified Duo Push Universal Promptissa. Microsoft Entran ehdollisen pääsyn ominaisuuden avulla voidaan luoda sääntöjä, jotka arvioivat Entra ID:n käyttäjien pyrkimyksiä käyttää sovelluksia ja sallia pääsyn vain, kun tietyt ehdot täyttyvät, kuten käyttäjäryhmän jäsenyys, maantieteellinen sijainti tai onnistunut monivaiheinen todentaminen. Vahvan toissijaisen todentamisen näille kirjautumisille tarjoaa Duon mukautettu Microsoft Entra ehdollisen pääsyn -hallinta,

joka parantaa ja laajentaa Azuren käyttörajoituksia. Entra ID P1- tai P2-jäsenyys tarvitaan ehdolliseen käyttöön kolmannen osapuolen mukautetuilla MFA-ohjaimilla, ja on erittäin tärkeää varmistaa Microsoft-tilauksen ominaisuudet ennen kuin jatkaa käyttöönottoa. (Duo Two-Factor Authentication for Microsoft Entra ID (formerly Azure Active Directory) 2023.)

Microsoft Entran mukautetulle ohjaukselle on asetettu rajoituksia, varsinkin monivaiheisen todentamisen vaatimuksia koskevia rajoituksia, jotka eivät salli mukautettuja ohjausobjekteja. Microsoftin ehdollisen pääsyn käyttö ei tue monivaiheista todentamista, kun todentaminen tehdään mukautetulla ohjausobjektilla, kuten Duolla. Tämä osoittaa, että mukautetut ohjausobjektit eivät voi täyttää ehdollisen pääsyn sääntöä, joka vaatii monivaiheista todentamista. Tietyissä skenaarioissa, kuten kun Microsoft Entra ID tai Microsoft 365 on yhdistetty Duo Single Sign-On-sovellukseen tai Azure Microsoft AD FS:n kanssa Duo MFA voi täyttää ehdollisen pääsyn monivaiheiset vaatimukset. Jälkimmäisessä tapauksessa Duon asennus AD FS:lle ja konfiguraatio ovat välttämättömiä MFA-todentamismenetelmän viittausvaatimuksen välittämiseksi takaisin Entra ID:lle. Lisäksi Duon mukautettu ohjaus ei ole käytettävissä Duo Federal -suunnitelmissa, koska Azure Government ei vielä salli mukautettuja ohjausobjekteja ehdollisissa käyttöoikeuksissa. Tämä edellyttää Azure Government -versioiden tutkimista Entra ID:n Premium -ominaisuuksissa. On tärkeää muistaa, että Microsoft Entran ehdollisen pääsyn kautta suojataan pilvisovellukset, jotka ovat käytettävissä verkkoselaimilla tai työpöytä- ja mobiiliasiakasohjelmilla, mikäli ne tukevat Microsoftin modernia todentamista, kuten Office 2016 ja 2019. Sen sijaan Office-asiakkaille, jotka eivät tue modernia todentamista, kuten Office 2010 tai sitä vanhemmat versiot, suojaa ei taata. Koska Microsoft hyödyntää ehdollisen pääsyn käytäntöjä, kolmannen osapuolen MFA:n asentaminen ei ole mahdollista. Sen sijaan Duon mukautuva MFA-hallinta integroituu tehokkaasti Microsoftin nykyisiin todentamismenetelmiin tarjoten joustavaa ja turvallista käyttöä. Ehdollisen pääsyn avulla on mahdollista estää vanhentuneiden Office-asiakkaiden todentaminen, jotka eivät tue nykyisiä todentamismenetelmiä. (Duo Two-Factor Authentication for Microsoft Entra ID (formerly Azure Active Directory) 2023.)

5.4 Käytännöt

Organisaatiot käyttävät yleensä porrastettua käyttöönottostrategiaa toteuttaessaan Duon Trusted Endpoints -käytäntöä sujuvan integraation varmistamiseksi. Duon sisäisen selaimen todentamiskehotteen avulla testaavan sovelluksen valitseminen on toimenpiteen ensimmäinen vaihe, joka on

olennainen päätepisteen hallitun tai hallitsemattoman tilan raportoinnissa. Seuraava vaihe sisältää Duo-ryhmän tunnistamisen tai luomisen pilottikäyttäjien kanssa. Käyttäjien, jotka käyttävät Microsoft Entra Connect -hakemistosynkronointia tai AD-hakemistosynkronointia on ensin rakennettava tämä pilottiryhmä lähdehakemistoonsa, lisättävä testijäseniä ja synkronoitava se sitten Duoon. Sen jälkeen luodaan täysin uusi Trusted Endpoints -käytäntö, joka sisältää hallinnan integrointiasetukset laitehallinnan tilan seurantaa ja raportointia varten. Tämä käytäntö toteutetaan testaussovelluksen pilottiryhmän hallinnan integroinnin aktivoinnin yhteydessä. Seuraavana käytäntönä on seuranta. Essentials -version asiakkaat voivat seurata Authentication Logs -raporttia nähdäkseen käyttäjien todentamisia luotetuista päätepisteistä, kun taas Duo Premier- ja Duo Advantage -sopimusten käyttäjiä kehotetaan hyödyntämään Device Insight- ja Endpoints-ominaisuuksia Duon hallintapaneelissa. Pilottikäyttäjien päätepisteet alkavat ilmoittaa Duolle heidän valvotusta tilastaan heti todentamisen jälkeen. Lopuksi lisäämällä käytäntö yleiseen käytäntöön se on kaikkien käyttäjien ja ohjelmien saatavilla. Jotta sen tietoturvapotentiaali voidaan hyödyntää täysimääräisesti, valinnainen vaihe on käyttää Trusted Endpoints -käytäntöä, joka estää pääsyn arkaluonteisiin sovelluksiin. (Duo Trusted Endpoints 2023.)

5.4.1 Käytäntöjen integrointi

Duon Trusted Endpoints -käytäntö tarjoaa monivaiheisen todentamisen integrointia osaksi Cisco Duon tarjoamaa kokonaisratkaisua. Tämä integroituvuus tekee Cisco Duosta tehokkaan ja monikäyttöisen ratkaisun organisaation tietoturvavaatimuksiin. Se mahdollistaa yhdenmukaisen turvallisuuden useilla eri alustoilla ja palveluissa samalla, kun se tarjoaa käyttäjille mahdollisuuden käyttää organisaation resursseja helposti ja turvallisesti.

Cisco Duo on suunniteltu integroitumaan saumattomasti monenlaisten palveluiden, sovellusten ja tietojärjestelmien kanssa organisaation tarpeiden mukaan. Tämä tarkoittaa sitä, että organisaatiot voivat ottaa käyttöön Cisco Duon monivaiheisen todentamisen eri osa-alueilla. Cisco Duo voidaan integroida VPN-yhteyksiin, mikä mahdollistaa turvallisen etäyhteyden organisaation verkkoon. Käyttäjät voivat todentaa henkilöllisyytensä ennen kuin he saavat pääsyn verkkoon. Organisaatiot voivat integroida Cisco Duon verkkosovelluksiin, kuten sähköpostiin tai intranet-sivustoihin. Tämä tarkoittaa sitä, että käyttäjät joutuvat vahvistamaan henkilöllisyytensä ennen kuin he voivat käyttää näitä sovelluksia. Cisco Duo voidaan myös integroida pilvipalveluihin, kuten Microsoft Entraan tai AWS:ään. Tämä varmistaa, että käyttäjien on todennettava henkilöllisyytensä ennen kuin he

voivat käyttää organisaation tallennustilaa tai muita pilvipalveluita. (Remote Access Integrations n.d.)

5.4.2 Käytäntöjen luominen

Uuden käytännön luominen, joka on tarkoitettu vain luotetuille päätepisteille, edellyttää, että se on asetettu tarkistamaan päätepisteiden hallinnan tila ennen Trusted Endpoints -käytännön soveltamista sovelluksiin ja ryhmiin. Tämä prosessi alkaa, kun siirrytään Duon hallintapaneeliin käyttäen järjestelmänvalvojan tunnuksia, joilla on omistajan tai järjestelmänvalvojan oikeudet. Ohjelma, jota halutaan pilotoida Trusted Endpoints -käytännöllä, valitaan navigoimalla sen luokse. Tämän jälkeen "Käytä käytäntöä käyttäjäryhmille" -vaihtoehto valitaan uuden käytännön määrittämiseksi valitulle pilottiryhmälle. Uusi käytäntö voidaan luoda valitsemalla sopiva linkki, joka avaa tyhjän käytäntöeditorin, jotta voidaan toteuttaa mukautettu lähestymistapa. Käytännölle annetaan kuvaava nimi, valitaan Luotetut päätepisteet -käytäntökohde ja määritetään "Salli kaikki päätepisteet". Käytännön luominen finalisoidaan "Luo käytäntö" -vaihtoehdolla, joka tallentaa asetukset ja palaa takaisin "Käytä käytäntöä" -näkymään, missä äskettäin luotu Trusted Endpoints -käytäntö on valittuna. Tämä käytäntö voidaan lisäksi kohdentaa tiettyyn ryhmään lisäämällä pilottiryhmän nimi Ryhmät-kenttään, valitsemalla se luettelosta ja napsauttamalla "Käytä käytäntöä". Tämän toimenpiteen seurauksena sovellussivu päivittyy näyttämään uuden ryhmäkäytäntöasetuksen. (Duo Trusted Endpoints 2023.)

5.5 Duo Trusted Endpoints -käytäntö

Ciscon Duo Trusted Endpoints -käytäntö helpottaa luotettujen päätepisteiden luomista ja hallintaa, mikä lisää yrityksen turvallisuutta. Tämä ominaisuus helpottaa suojatun pääsyn myöntämistä yrityksesi käyttämille sovelluksille käyttämällä käytäntöjä, jotka tehostavat järjestelmän turvallisuutta tekniikoiden avulla, kuten laitevahvistukset, sovelluksen autentikointi ja hallintatila. Duolla on ratkaiseva rooli, kun voit erottaa hallitut ja hallitsemattomat päätepisteet, jotka pääsevät käyttämään selainpohjaisia sovelluksiasi. Trusted Endpoints -käytäntö on välttämätön sen valvomiseksi, onko näitä sovelluksia käyttävien asiakkaiden tunnustettu hallituiksi. Sillä on myös kyky estää pääsy hallitsemattomista järjestelmistä. Tämä olennainen suojauskäytäntö on osa Duon täydellisiä tietoturvapalveluja, ja se sisältyy Duo Essentials-, Duo Advantage- ja Duo Premier -pakettei-

hin. Trusted Endpoints -käytäntö on perustunut ennen myös varmenteeseen, mutta se on poistumassa lähiaikoina, joten jäljelle on jää vielä Duo Desktopin tai Duo Mobilen avulla tapahtuva varmennus. (Duo Trusted Endpoints 2023.)

Windows- sekä macOS-laitteissa Duo Desktop parantaa huomattavasti tietoturvaa selainpohjaisiin sovelluksiin kirjautuessa. Kun Duo Desktop on asennettu päätepisteeseen, se palauttaa huolellisesti yksilölliset tiedot, kuten konetunnukset Duolle interaktiivisen kehotteen ilmestyessä. Tämä on välttämätöntä luotettujen päätepisteiden hallintaintegraatioissa, koska ne vertaavat näitä tietoja päätepisteiden hallintajärjestelmän tietoihin tietokoneen hallintatilan määrittämiseksi. Nämä integraatiot perustuvat Duo Desktopiin vahvistusta varten. Vastaavasti Duo Mobilea käytetään todentamisen yhteydessä Duon suojattuihin sovelluksiin Android- tai iOS-laitteista. Täällä Duo etsii laitteelta Duo Mobile -sovellusta, joka on olennainen vaihe päätepisteen hallintatilan selvittämisessä. Tämä menetelmä on olennainen Duon suunnitelmassa taata säännelty ja turvallinen käyttö useilla alustoilla ja ylläpitää vahvaa tietoturvaa sekä pöytäkone- että mobiiliasetuksissa. (Duo Trusted Endpoints 2023.)

5.5.1 Duo Desktop

Duo Desktop parantaa organisaation hallintaa yrityksen sovellusten käyttöoikeuksissa arvioimalla kannettavien ja pöytätietokoneiden suojausasennon tai vahvistamalla, että Duo Desktop on läsnä päätepisteessä. Se koostuu kolmesta pääosasta, jotka ovat natiivi asiakassovellus Windowsille, Linuxille ja macOS:lle, mitkä varmistavat päätepisteen suojausasennon Duon suojaaman sovelluksen käyttäjän todentamisen aikana sekä muita päätepistetietoja, joita voidaan käyttää Duon hallintapaneelin kautta ja Duon käyttöoikeuskäytännöt, jotka pakottavat sovellusten käyttöoikeuden päätepisteen kunnon perusteella. Käyttäjiä pyydetään lataamaan ja asentamaan Duo Desktop, kun he kirjautuvat ensimmäisen kerran sovellukseen, joka on suojattu Duo Desktop -käytännöllä. Asennuksen jälkeen Duo Desktop -käytännön mukaan epäterveitä päätepisteitä estetään kirjautumasta sisään selainpohjaisen todentamiskehotteen kautta, ja käyttäjille ilmoitetaan hylkäämisen syystä. Ohjelma opastaa käyttäjää vahvistamaan päätepisteen tietoturvatasoa, jos se ei vastaa Duo Desktop -käytännön turvallisuusstandardeja. Turvallisuushuolia kuitenkin on sillä, vaikka hankitut tiedot siirretään turvallisesti Duo Desktopin kautta niitä ei voida yksilöidä, mikä tekee niistä alttiita

häikäilemättömien osapuolten sieppaamiselle ja keksimiselle. Käyttäjänä esiintyminen on epätodennäköisempää, kun käytetään yksilöllisiä todentamistunnuksia. Päätepisteen rekisteröinnin ottaminen käyttöön voi vähentää tätä vaaraa entisestään. (Duo Desktop 2023.)

Duo Essentials-, Advantage- tai Premier-tilaus, järjestelmänvalvojan käyttöoikeudet Duon hallintapaneeliin ja käyttäjien päätepisteet sisältäen Windows, Linux ja macOS, joissa on suora tai HTTP-välityspalvelin yhteys Duo Securityn palveluun ovat Duo Desktopin käyttöönoton edellytyksiä. Päätepisteen rekisteröintiä varten tuetuissa päätepisteissä tulisi mieluiten olla Secure Enclave Macissa tai TPM 2.0 Windowsissa. Tietyt Linux-jakelut, macOS 10.15 ja uudemmat, Windows 10 build 1803 ja uudemmat sekä Windows 11 ovat tuettuja käyttöjärjestelmiä. Erityisesti Duo Desktop ei tue macOS:n betaversioita, Windows Server -versioita, aiempia Windows-versioita, kuten Windows 7 tai 8.1, ja virtuaalikoneita, joissa on sekä Windows että macOS. (Duo Desktop 2023.)

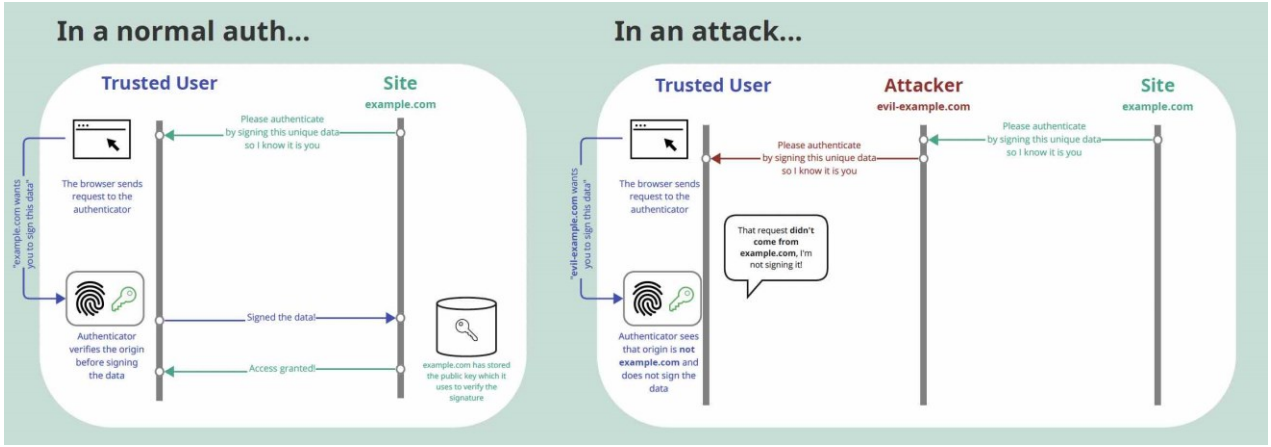
5.6 Monitorointi ja seuranta

Koska Device Insight- ja Endpoints-sivut ovat vain Duo Premier- tai Duo Advantage -sopimuksia tehneiden yritysten käytettävissä, luotettujen päätepisteiden seuranta on tärkeä osa verkon tietoturvan hallintaa. Duon kehote ei näytä muuttuvan, kun käyttäjät vierailevat Duon Trusted Endpoints -käytännön kattamissa sovelluksissa, mutta Duo määrittää huomaamattomasti ohjataanko päätepisteitä. Tämän arvioinnin tulokset näkyvät Duon hallintapaneelissa. Erityisesti laitevarmenteen tila ilmenee "Kyllä"-arvona päätepisteille, jotka ovat hyväksytysti suorittaneet Duon hallinnoidun järjestelmän tarkistuksen. Vastaavasti, ne päätepisteet, jotka eivät läpäise tarkistusta, saavat "Ei"-arvon. Tämä tieto on nähtävissä Trusted Endpoint -sarakkeessa Endpoints-sivulla, sekä päätepisteen ja käyttäjän omilla tietosivuilla. Päätepiste ei ole vielä käyttänyt Trusted Endpoints -käytännön kattamaa sovellusta, jos sen tila on ”Tuntematon” Trusted Endpoint -sarakkeessa. Lisäksi Duo näyttää muita päätepistetietoja sekä varmenteen myöntämispäivämäärää, jos se voi varmistaa nämä tiedot. Päätepisteet-taulukko voidaan suodattaa varmenteen vanhenemisen mukaan, jotta voidaan helpottaa ennakoivaa laitevarmenteiden hallintaa ja varmistaa, että Trusted

Endpoints -käytäntöä noudatetaan. Termi "pian" tarkoittaa, että varmenne lähestyy uusimisikkunaansa, joka on kolme päivää yhden viikon varmenteilla ja kaksi viikkoa yhden vuoden varmenteilla. (Duo Trusted Endpoints 2023.)

5.7 AiTM-hyökkäys

Golden (2024) kuvaa, että yleisesti Attack-in-the-Middle hyökkäyksessä alkuun kuuluu usein huijausviesti, jonka hyökkääjä lähettää kohteelle sisältäen haitallisen linkin. Hyökkääjän päätavoitteena on saada viestin vastaanottaja klikkaamaan tätä linkkiä. Mielenkiintoista on, että usein käyttäjän ei edes tarvitse paljastaa salasanaansa. Linkkiä klikkaamalla käyttäjä ohjataan proxy-palvelimelle, joka näyttää hämmästyttävän samanlaiselta kuin aito verkkosivu, eroten lähinnä URL-osoitteessa. Hän korostaa, että monet näistä huijaussivustoista saattavat silti näyttää turvallisuuslukon kuvaketta, koska ne käyttävät HTTPS-protokollaa, mikä voi johtaa käyttäjän harhaan ajattelemaan sivuston olevan turvallinen. Proxy-sivuston keskeinen ominaisuus on, että se mahdollistaa hyökkääjälle käyttäjän voimassa olevien istuntotunnusten istunnon evästeet anastamisen. Tämä on merkittävää, koska se antaa hyökkääjälle mahdollisuuden ohittaa tavallinen kirjautumisprosessi ja päästä luvattomasti käsiksi järjestelmiin ilman käyttäjän varsinaisia kirjautumistietoja niin kuin kuviossa 9 esitetään. (Golden 2024.)



Kuvio 9. Normaali todentaminen ja AiTM-hyökkäys (Golden 2024)

Kun hyökkääjät sijoittavat itsensä verkkoon kytkettyjen laitteiden väliin, he pystyvät toteuttamaan useita vaarallisia toimia. Tällaisia toimia ovat esimerkiksi toistohyökkäykset, joiden avulla he voivat

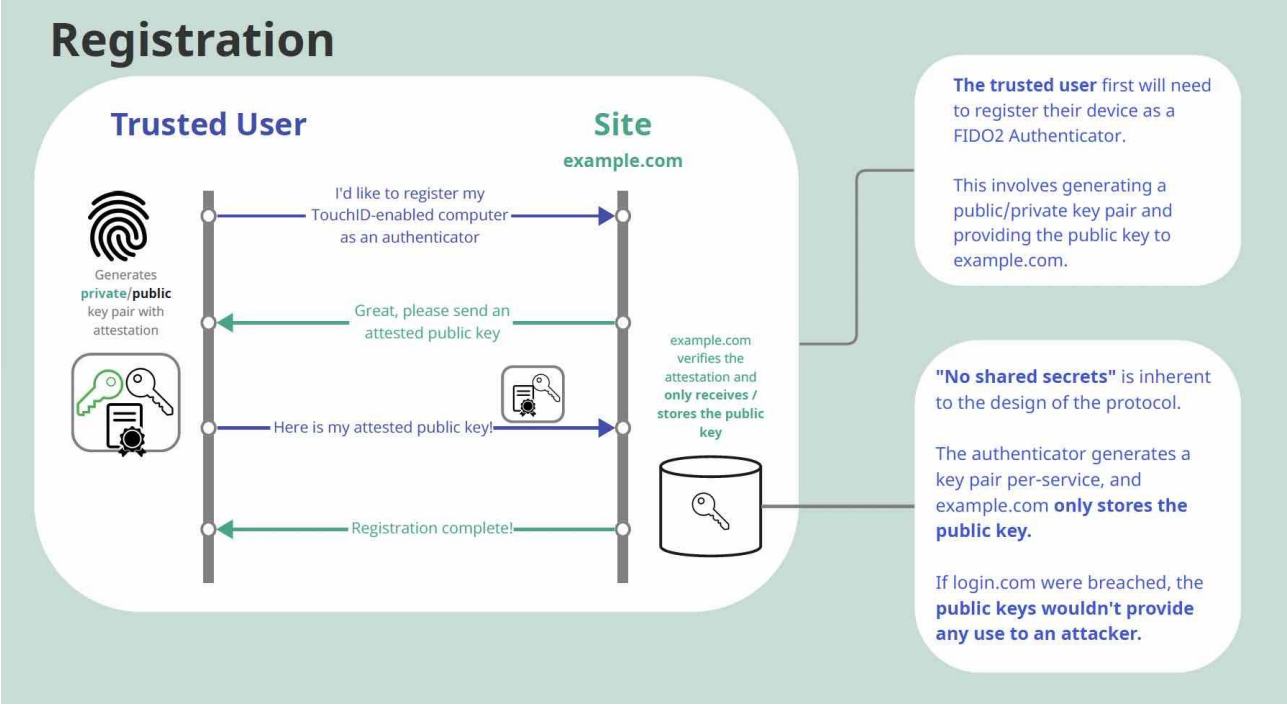
käyttää hyväksi valtuutustietoja, manipuloida siirrettyjä tietoja sekä nuuskia verkossa liikkuvaa tietoa. Nämä hyökkäykset mahdollistavat heille pääsyn arkaluonteisiin tietoihin ja tietoliikenteeseen, mikä voi johtaa merkittäviin tietoturvariskeihin ja tietojen vuotoihin. He käyttävät suosittuja verkkoprotokollia mukaan lukien ARP, DNS ja LLMNR laiteyhteyden uudelleenreitittämiseen hallitsemansa järjestelmän kautta, mikä antaa heille mahdollisuuden kerätä tietoja tai suorittaa muita haitallisia toimia. AiTM-asemien määrittämiseksi vastustajat voivat esimerkiksi muokata uhrien DNS-asetuksia estääkseen tai uudelleen reitittääkseen pääsyn luotettaville verkkosivustoille, levittää haittaohjelmia, siepata valtuustietoja ja istuntoevästeitä tai suorittaa alenevia hyökkäyksiä neuvottelemalla vähemmän turvallisista protokollaversioista kuten SSL/TLS tai heikompia salausalgoritmeja. (Adversary-in-the-Middle 2023.)

5.7.1 AiTM-hyökkäykseltä puolustautuminen

Kaikkia monivaiheisen todentamisen ratkaisuja ei tehdä tasa-arvoisiksi jatkuvasti kehittyvässä kyberturvallisuuden maailmassa, koska tietojenkalastelumenetelmät muuttuvat jatkuvasti ja kohtaavat vakiintuneita MFA-järjestelmiä. Cisco Duo, joka on MFA:n ja kulunvalvonnan edelläkävijä loi tietojenkalastelut kestävän MFA:n, ja CISA pitää sitä parhaana saatavilla olevana MFA:na. Tämä parannettu monivaiheinen todentaminen eliminoi salasanojen tarpeen käyttämällä FIDO2-todentamistekniikoita ja ei-kalastettavissa olevia valtuustietoja, jotka yhdistävät fyysisen ominaisuuden, kuten älypuhelimen luontaiseen ominaisuuteen, kuten sormenjälkeen. Verified Duo Push on Cisco Duon kehittämä toiminto, joka parantaa turvallisuutta vaatimalla käyttäjiltä vahvistuskoodin lähettämistä todentamispyyntöihin. Tämä ominaisuus pienentää virheellisten käyttöoikeuksien myöntämisen riskiä ja sisältää petosraportointityökalun uhkien monitorointiin. Sen kehityksen taustalla on pyrkimys torjua push-ilmoituksiin kohdistuvia hyökkäyksiä sekä vähentää monivaiheisen todentamisen aiheuttamaa väsymystä käyttäjissä. SAML- ja WebAuthn-protokollien tukema Cisco Duo parantaa MFA:ta entisestään ominaisuuksilla, kuten tekijöiden valinnalla, luotetuilla päätepisteillä, riskipohjaisilla muistetuilla päätepisteillä ja päätepisteen kunnon varmistuksella. Lisäksi alusta kannustaa vahvaa itsepalvelu MFA:ta, mikä vähentää IT-osaston työmäärää sallimalla käyttäjien rekisteröityä itse ja hallita todentamismenetelmiään Duo Self-Service Portalin avulla. Lisäksi SAML v2.0:n, OpenID Connectin ja AWS Verified Accessin tukemisen ansiosta Cisco Duon integrointi SSO-sisäänkirjautumisen kanssa parantaa yritysturvallisuutta ja käyttömukavuutta.

Tämä antaa organisaatiolle mahdollisuuden laajentaa vankkaa monivaiheista todentamista ja luotettuja käyttöoikeuksia pitäen se jatkuvasti kehittyvän kyberturvallisuusympäristön edellä. (Not All MFA Solutions Are Created Equal n.d.)

Golden (2024) esittelee edistyneen tietojenkalastelulta suojatun todentamismenetelmän kuviossa 10, joka käyttää julkisen avaimen kryptografiaa. Tässä menetelmässä yksityinen avain tallennetaan käyttäjän laitteeseen, kun taas julkinen avain rekisteröidään sovellukseen. Käyttäjän todentautuessa yksityisellä avaimella se pysyy laitteessa suojaten sitä varastamiselta. Hänen mukaansa selaimen lähettämä alkuperätieto ja tunnistautumistietojen sidonta alkuperäiseen istuntoon lisäävät turvallisuutta tarjoten vahvan suojan tietojenkalastelua vastaan. (Golden 2024.)



Kuvio 10. Cisco Duon tietojenkalastelulta suojattu todentaminen (Golden 2024

Todentamisen alkuperän tarkistus FIDO2-todentamisessa, kuten Golden (2024) kuvaa, sisältää selaimen lähettämän alkuperätiedon siirron turva-avaimelle tai puhelimelle, joka varmistaa pyynnön aitouden. Tämä suojaa käyttäjiä URL-osoitteiden hienovaraisilta manipulaatioilta. Tokenin sidonta tässä yhteydessä antaa laitteelle väliaikaisen tunnisteen, mikä estää AiTM-hyökkääjien pääsyn tietoihin, koska ne ovat sidoksissa alkuperäiseen turvalliseen istuntoon. (Golden 2024.)

Goldenin (2024) mukaan Duon salasanaton ratkaisu hyödyntää FIDO2-standardeja, jolloin käyttäjät voivat todentaa itsensä ilman salasanoja käyttämällä biometrisiä tunnisteita tai turva-avaimia. Tämä yksinkertaistaa monivaiheista todentamista. Duo tukee myös WebAuthn-tunnisteita yksityisten avainten synkronointiin laitteiden välillä. Organisaatiot voivat vahvistaa turvallisuutta yhdistämällä laitetunnistuspolitiikka, vahvan todentamisen ja Duo Desktopin Trusted Endpoints -käytännöt, kuten automaattinen rekisteröinti, mitkä parantavat suojaa entisestään. (Golden 2024.)

5.7.2 AiTM-hyökkäyksen testaaminen

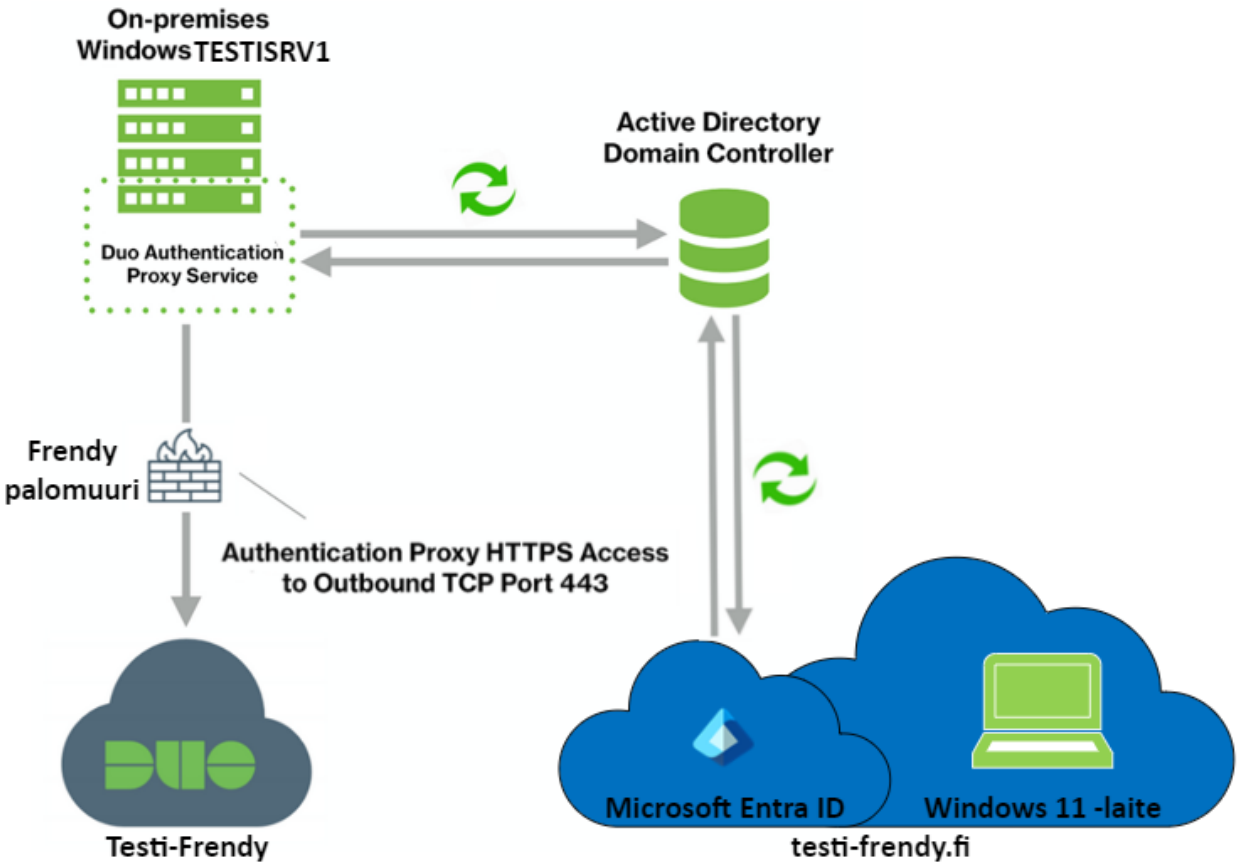
Tarkasteltiin AiTM-hyökkäyksen testausta Cisco Duossa, joka ei mahtunut tämän työn aikatauluun vaan jäi suunnittelun jälkeen kesken, mutta tätä tullaa jatkamaan Frendylla myöhemmin loppuun. Tarkastelussa oleellisena on, miten tämä monivaiheisen todentamisen järjestelmä voi suojata käyttäjiä aktiivisen hyökkäyksen muodossa, jossa hyökkääjä pyrkii välimiehenä kaappaamaan ja manipuloimaan tiedonsiirtoa kahden osapuolen välillä. Testaus keskittyy erityisesti siihen, kuinka Duo voi tunnistaa ja estää tällaiset hyökkäykset varmistaen käyttäjien todentamistietojen turvallisuuden ja ehkäisten luvattoman pääsyn järjestelmiin. Erityistä huomiota kiinnitetään Duon kykyyn estää luvaton pääsy ja varmistaa, että käyttäjien todentamiset ovat turvallisia, vaikka ne altistuisivat AiTM-hyökkäykselle. Tämä lähestymistapa ei ainoastaan korosta Duon teknisen suojauksen merkitystä, vaan myös sen roolia laajemmassa tietoturvakulttuurissa, jossa jatkuva valppaus ja hyökkäysmenetelmien ymmärtäminen ovat avainasemassa.

Evilginx on kehittynyt hyökkäystyökalu, joka mahdollistaa sisäänkirjautumistietojen ja istuntoevästeiden kaappaamisen kiertäen näin kaksivaiheisen ja monivaiheisen todentamisen. Se julkaistiin vuonna 2017 seuraajana alkuperäiselle versiolle, joka perustui nginx HTTP-palvelimen muokattuun versioon. Uusin Evilginx on kehitetty GO-ohjelmointikielellä ja sisältää omat HTTP- ja DNS-palvelimensa, mikä tekee sen käyttöönotosta ja käytöstä vaivatonta. (Evilginx 3.0 2018.)

6 Ympäristön esittely

Kuviossa 11 esitetään työssä käytössä ollut ympäristö. Opinnäytetyön ympäristön lähtökohtana oli Internet, josta käyttäjät pääsevät ympäristöön. Ympäristön suojauksesta ja pääsyn valvomisesta vastaa Frendyn palomuuri, joka suodattaa liikenteen molempiin suuntiin, missä sallitaan todentamisvälityspalvelimen HTTPS-pääsy ulospäin TCP-porttiin 443. Ympäristöön kuuluu isona osana

Frendyn testiympäristön fyysinen Windows Server -pohjainen TESTISRV1-palvelin ja siellä sijaitseva Active Directory -ohjain, joka sisältää käyttäjätiedot, ryhmät ja muita todentamiseen liittyviä tietoja. Käyttäjissä ja ryhmissä määritellään käyttäjäoikeudet ja ryhmäkäytännöt sekä lisäksi palvelimelle on konfiguroitu Duo Authentication -todennusvälityspalvelin Cisco Duon monivaiheista todentamista varten. Palvelimella on käytössä LDAP-synkronointi, joka välittää käyttäjätietoja palvelimen ja Cisco Duon välillä. Ympäristöön kuuluu vielä Frendyn testiympäristön Microsoft Entra -vuokralainen, johon Active Directory -ohjaimelta tulevat tiedot synkronoidaan Microsoft Entra Connectin avulla ja käyttäjille saadaan määritettyä Microsoft 365 -lisenssit Microsoft Entra ID:ssä. Monivaiheisen todentamisen palveluita tarjoava Cisco Duo pitää sisällään sinne testikäyttöä varten määritetyn Testi-Frendy-tilin, minne on tuotu Microsoft Active Directorysta käyttäjätiedot synkronoinnin kautta.



Kuvio 11. Opinnäytetyön ympäristön topologia

Cisco Duon hallintapaneeliin luodaan Microsoft Azure Active Directory -sovelluksen suojaus niiden käyttäjien monivaiheisen todentamisen pakotusta varten, mitkä kuuluvat Frendyn testiympäristön

Microsoft Entra ID:seen ja seuraavaksi lisätään Cisco Duon hallintapaneeliin kautta Intune with Duo Desktop integraatio, jolla varmistetaan kirjautumisessa olevien päätepisteiden luotettavuus lukemalla suoraan Microsoft Entra ID:ltä päätepisteiden tiedot. Testaamisen käytetään uusimmalla Windows 11 -käyttöjärjestelmällä olevaa päätepistettä, joka on yhdistetty Frendyn testiympäristön Microsoft Entra -vuokralaiseen. Kyseisellä päätepisteellä pystytään testaamaan ja varmistamaan Cisco Duo MFA:n normaalia kirjautumista, mutta myös Cisco Duon Trusted Endpoints -käytännön kanssa olevaa kirjautumista sekä siihen liittyvää Duo Desktop -integraation ja sen sovelluksen toimintaa.

7 Toteutus

Työn toteutusvaiheessa korostui erityisesti eri järjestelmien välisten yhteyksien ja yhteensopivuuden merkitykset. Onnistuneen integraation avain oli syvällinen ymmärrys kunkin alustan teknisistä ominaisuuksista ja niiden mahdollistamista tietoturvaratkaisuista. Tämä edellytti yksityiskohtaista suunnittelua toimeksiantajan kanssa ja testausta varmistamalla, että jokainen komponentti toimi saumattomasti yhteen tarjoten sekä korkean tason tietoturvaa että optimaalista käytettävyyttä loppukäyttäjille. Tämän lisäksi projektin aikana kiinnitettiin huomiota järjestelmien skaalautuvuuteen, jotta ne voisivat mukautua organisaation kasvaviin tarpeisiin ja tuleviin teknologisiin muutoksiin. Valittujen teknologioiden pohjalta toteutettiin yleisluontoinen suunnitelma toteutuksen olennaisimmista ominaisuuksista. Toteutuksen kannalta keskeiset teknologiat valittuamme laadimme niiden perusteella yleisluonteisen suunnitelman, joka kuvasti projektin olennaisimpia ominaisuuksia. Tämä suunnitelma toimi perustana sille, miten eri teknologiset ratkaisut yhdistettäisiin saumattomasti samalla varmistaen, että kunkin teknologian ainutlaatuiset edut ja toiminnot tukevat projektin yleisiä tavoitteita ja vaatimuksia. Tämä lähestymistapa mahdollisti joustavan ja tehokkaan toteutusprosessin, jossa kunkin valitun teknologian rooli ja merkitys otettiin huolellisesti huomioon.

7.1 Pääjärjestelmät

Toteutuksen ytimessä oli useiden erilaisten teknologisten ratkaisujen yhdistäminen, mikä edellytti laajan ymmärryksen niin laitteistosta kuin ohjelmistoistakin. Tämän luvun alaosioissa mainitut teknologiat ovat keskeisessä roolissa teknisessä toteutuksessamme. Nämä teknologiat on valittu huo-

lellisesti, ja kunkin valinnan taustalla olevat perustelut on esitetty näissä alaluvuissa. Käytetyt teknologiat edustavat projektin ydinelementtejä, ja niiden valinta perustuu niiden merkitykseen ja soveltuvuuteen projektin tavoitteiden saavuttamiseksi.

7.1.1 Cisco Duo

Cisco Duo on kattava tietoturva-alusta, joka tarjoaa asiakkaille, liikekumppaneille ja työntekijöille kaiken kattavan identiteettipohjaisen suojan. Se tarjoaa erilaisia turvatoimia eri hinnoittelupisteissä ja sopii erikokoisille yrityksille. Duo tarjoaa suojatun SSO-kirjautumisen, alkeellisen valvonnan sekä työpöytä- ja mobiilikäyttösuojauksen pienille ja keskisuurille yrityksille. Pienten yritysten käytettävissä olevien ominaisuuksien lisäksi yritysversio tarjoaa etäkäyttöratkaisuja, parannettua laiteanalytiikkaa, parannettua laitteiden näkyvyyttä ja mukautuvaa pääsynhallintaa. (Not All MFA Solutions Are Created Equal n.d.)

Monivaiheinen todentaminen on käyttäjän henkilöllisyyden todentamiseen turvallinen etäkäyttö paikan päällä oleviin sovelluksiin ja laiteluottamus varmistamalla, että kaikki laitteet noudattavat suojausvaatimuksia ja kertakirjautuminen helpon pääsyn moniin sovelluksiin ovat vain muutamia alueita turvallisuudesta, jotka Duon ominaisuudet kattavat. Mukautuvat pääsysäännöt mahdollistavat myös henkilökohtaisen pääsyn rajoittamisen käyttäjien töiden, sijainnin ja muiden tekijöiden mukaan. (Not All MFA Solutions Are Created Equal n.d.)

Duon monipuolisuuden ansiosta sitä voidaan käyttää useilla eri aloilla, kuten julkishallinnossa, vähittäiskaupassa, terveydenhuollossa, koulutuksessa, rahoituksessa ja lakialalla. Se kattaa tietyt tietoturvavaatimukset, kuten tietojenkalasteluhyökkäyssuojan ja nollaluottamustaktiikat. Erityisesti Duo tarjoaa vankan MFA-suojauksen tehokkuutta tinkimättä integroimalla sen koko ekosysteemeihin. Sen tavoitteena on virtaviivaistaa toimintaa ja vähentää kitkaa niin, että ylläpitäjät ja loppukäyttäjät voivat keskittyä organisaation tavoitteiden saavuttamiseen. Duon riskiperusteisen todentamisen ansiosta käyttäjien todentaminen helpottuu, mikä parantaa turvallisuutta ja tehokkuutta. (Not All MFA Solutions Are Created Equal n.d.)

7.1.2 Microsoft Entra ID

Microsoft Entra ID on kattava pilvipohjainen identiteetin ja pääsynhallintaratkaisu, joka on suunniteltu auttamaan työntekijöitä turvallisesti ja tehokkaasti käyttämään sekä sisäisiä että ulkoisia resursseja. Sen avulla on helppo muodostaa yhteyksiä lukuisiin ulkoisiin resursseihin, kuten Azure-portaaliin, Microsoft 365:een ja laajaan valikoimaan SaaS-sovelluksia samalla kun se tarjoaa pääsyn organisaation räätälöityihin pilvisovelluksiin ja yrityksen intranet-sovelluksiin. Microsoft Entra ID on avain Azure-identiteettipalveluiden ymmärtämiseen ja hallintaan, ja se erottuu selvästi Active Directorystä ollen korvaamaton väline erilaisissa organisatorisissa tehtävissä. IT-päälliköt luottavat Microsoft Entra ID:hen resurssien ja sovellusten käytön valvomiseksi liiketoiminnan vaatimusten mukaisesti, mikä sisältää käyttäjähallinnan yksinkertaistamisen Windows Server AD:n ja pilvisovellusten, kuten Microsoft 365:n välillä sekä monivaiheisen todentamisen käyttöönoton kriittisten liiketoimintaresurssien suojaamiseksi. Sovelluskehittäjät voivat parantaa käyttökokemusta integroimalla kertakirjautumisen sovelluksiinsa käyttäen Microsoft Entra ID:tä, joka on standardien mukainen todentamispalvelu. Lisäksi Microsoft Entran sovellusliittymien avulla voidaan luoda räätälöityjä käyttökokemuksia hyödyntämällä yritystietoja. (What is Microsoft Entra ID? 2023.)

Microsoft Entra ID on ominaisuus, joka sisältyy Microsoft 365-, Office 365-, Azure- ja Dynamics CRM Online -tilauksiin. Tämän avulla käyttäjät voivat tehokkaasti hallita pääsyä linkitettyihin pilvisovelluksiin. Microsoft Entra ID tarjoaa joukon lisenssivaihtoehtoja vastatakseen eri organisaatioiden erilaisiin vaatimuksiin. Perusidentiteetin ja pääsynhallintatoiminnot, kuten hakemistosynkronointi, käyttäjien ja ryhmien hallinta sekä kertakirjautuminen eri alustoihin sisältyvät ilmaiseen versioon. Etuoikeutettu identiteetin hallinta tarjoaa laajan hallinnan järjestelmänvalvojan käyttöoikeuksiin, sillä Microsoft Entra ID -suojauksen riskiperusteiseen ehdolliseen käyttöön ja kehittyneeseen hallintaan kuuluvat P1- ja P2-lisenssien parannetut ominaisuudet. Lisäksi on olemassa käytön mukaan maksettavat -lisenssit, kuten Microsoft Entra B2C, jotka tarjoavat erityisiä identiteetin ja käyttöoikeuksien hallintaratkaisuja sovelluksille, jotka ovat vuorovaikutuksessa asiakkaiden kanssa. (What is Microsoft Entra ID? 2023.)

Microsoft Entra ID -lisenssin valitseminen avaa joukon ominaisuuksia, jotka jakautuvat eri luokkiin ja, jotka kaikki on tarkoitettu parantamaan turvallisuutta ja yksinkertaistamaan yrityksesi digitaalisen ympäristön hallintoa. Sovellusten välityspalvelimen, kertakirjautumisen, My Apps -rajapinnan

ja SaaS-sovellusten hallinnan integroinnin avulla hallintaa helpottavat sovellusten hallintaominaisuudet mahdollistavat sekä paikallisten että pilvipohjaisten sovellusten hallinnan. Ominaisuudet, kuten monivaiheinen todentaminen, mittatilaustyönä tehdyt kiellettyjen salasanojen luettelot, itsepalvelusalasanojen nollaukset ja älykkäät lukitusmekanismit ovat välttämättömiä todentamisen maailmassa. Microsoft Entra ID tarjoaa kehittäjille työkaluja Microsoft Graphia ja muita sovelluslIittymiä käyttävien sovellusten luomiseen sekä Microsoft-identiteettien käyttöliittymään. Voit hallita onnistuneesti vierailevia käyttäjiä, ulkoisia kumppaneita ja asiakkaiden sitoutumista tämän ratkaisun avulla, joka hoitaa myös B2B ja B2C -vuorovaikutukset. Pilvisovellukset ja yrityksen tiedot ovat käytettävissä turvallisesti ja yhteensopivalla tavalla ehdollisen käytön ja laitehallinnan ansiosta. Lisäksi ominaisuudet, kuten Hybrid Identity, Enterprise User Management ja Domain Services mahdollistavat helpon alustan hallinnan ja integroinnin. Organisaation identiteettien eheys ja turvallisuus ovat erityisesti identiteetin suojauksen ja identiteetin hallinnan aihe. Managed Identities for Azure -ympäristöt mahdollistavat automaattisen identiteetinhallinnan, ja PIM tarjoaa kaiken kattavan kulunhallinnan yrityksen sisällä. Lopuksi Workload Identities mahdollistaa ohjelmistojen työkuormien tehokkaan autentikoinnin ja palvelujen ja resurssien käytön, kun taas valvonta- ja terveysominaisuudet tarjoavat näkemyksiä tietoturva- ja kulutustrendeistä. Jokainen elementti on olennainen sen varmistamiseksi, että yritykselläsi on turvallinen, tehokas ja vaatimustenmukainen digitaalinen ekosysteemi. (What is Microsoft Entra ID? 2023.)

7.1.3 Microsoft Active Directory Domain Services

Verkon yhteydessä hakemisto on hierarkkinen rakenne, joka ylläpitää tehokkaasti tietoja eri verkko-objekteista. Yksi parhaista esimerkeistä hakemistopalvelusta on Active Directory Domain Services, joka tarjoaa edistyneitä tekniikoita näiden hakemistotietojen pitämiseen turvassa ja mahdollistaa verkon käyttäjien ja järjestelmänvalvojien pääsyn niihin. AD DS esimerkiksi pitää kirjaa tärkeistä käyttäjätilitiedoista, kuten nimistä, salasanoista ja puhelinnumeroista, ja helpottaa verkon valtuutettujen käyttäjien pääsyä niihin. (Active Directory Domain Services Overview 2022.)

Active Directoryn perusperustana on tietovarasto, joka järjestää hakemistotiedot loogisesti ja hierarkkisesti. Active Directoryn perustana oleva tietovarasto sisältää suuren joukon objekteja, mukaan lukien jaetut resurssit, kuten palvelimet, taltiot, tulostimet sekä tietokone- ja verkkotilit. Sisäänkirjautumisen todentamisen ja hakemisto-objektien pääsynhallinnan ansiosta Active Directory

-suojaus on integroitu saumattomasti, jolloin verkon käyttäjät voivat käyttää resursseja missä tahansa ja samalla järjestelmänvalvojat voivat hallita tietoja ja koko yritystä yhdellä kirjautumisella. (Active Directory Domain Services Overview 2022.)

Kaava on kokoelma sääntöjä, jotka määrittelevät objektityypit, ominaisuudet, rajoitukset ja nimeämiskäytännöt hakemiston sisällä. Se on yksi Active Directoryn pääosista. Toinen tärkeä osa on maailmanlaajuinen luettelo, joka auttaa järjestelmänvalvojia ja käyttäjiä löytämään hakemistotiedot eri toimialueista tarjoamalla yksityiskohtaisia tietoja kustakin hakemiston objektista. Lisäksi Active Directoryssa on tehokas kysely- ja indeksiarkkitehtuuri, joka helpottaa verkon käyttäjien ja sovellusten julkaisua ja etsintää kohteita ja niiden attribuutteja. (Active Directory Domain Services Overview 2022.)

Lopuksi Active Directoryn replikointitoiminto auttaa suuresti hakemistotietojen jakelua koko verkossa. Jokainen toimialueen ohjain osallistuu tähän replikointiprosessiin ja säilyttää kokonaisen kopion toimialueensa hakemistotiedoista. Tällä varmistetaan, että hakemistotietoihin tehdyt muutokset replikoidaan tarkasti ja johdonmukaisesti kaikkien toimialueen ohjauskoneiden kesken. (Active Directory Domain Services Overview 2022.)

7.2 Toiminnan kuvaus

Työ keskittyy Cisco Duo MFA:n käyttöönottoon Frendyn testiympäristössä, jossa keskeisenä tavoitteena on parantaa organisaation tietoturvaa ja käyttäjien todentamisprosesseja. Toteutuksessa otettiin huomioon Cisco Duon yhdistäminen olemassa oleviin järjestelmiin, kuten Active Directoryyn, ja sen toimivuus eri käyttäjän päätepisteiden kanssa. Työssä käsiteltiin asennuksen, konfiguraation ja testausprosessien yksityiskohtia, tarkasteltiin käyttäjäpalautetta sekä käyttöönoton strategioita. Cisco Duon tehokkuus erilaisten tietoturvariskien, kuten tietojenkalasteluhyökkäysten ehkäisyssä on myös arvioinnin kohteena. Opinnäytetyö tarjoaa kokonaisvaltaisen kuvauksen Cisco Duo MFA:n käyttöönotosta Frendyn IT-infrastruktuuriin, tietoturvaan ja käyttäjäkokemukseen.

Lisäksi työssä käytiin läpi, miten Cisco Duo MFA:n käyttöönotto vaikuttaa organisaation tietoturvapolitiikkaan ja käyttäjien päivittäiseen toimintaan. Tutkimus sisältää analyysin käyttöönotosta, kuten identiteetin synkronoinnista ja laitehallinnasta, sekä niiden ratkaisuista. Tarkastelussa on

myös, kuinka Duo MFA integroituu organisaation olemassa oleviin tietoturvakäytäntöihin ja millaisia vaikutuksia sillä on loppukäyttäjien todentamiskokemukseen. Työ pyrkii tarjoamaan suosituksia parhaille käytännöille ja strategioille Cisco Duon tehokkaaksi käyttöönotoksi ottaen huomioon sekä tekniset että käyttäjäkeskeiset näkökulmat.

Käyttöönoton aikana havaittiin, että Cisco Duon käyttöönotto parantaa merkittävästi organisaation tietoturvan tasoa tarjoamalla vahvemman todentamisen. Käyttäjäkokemuksen näkökulmasta Duo tarjosi sujuvan ja intuitiivisen kokemuksen, mikä helpotti uuden järjestelmän omaksumista. Tämä kokemus tarjoaa arvokasta tietoa ja oppeja Cisco Duon laajemmalle käyttöönotolle organisaatiossa.

7.3 Cisco Duo versioiden vertailut ja kustannukset

Cisco Duo on monivaiheisen todentamisen ja turvallisuuden hallintaratkaisu, joka tarjoaa erilaisia hinnoittelumalleja asiakkailleen. Kustannukset voivat vaihdella organisaation tarpeiden ja käytettävien ominaisuuksien mukaan. Duo tarjoaa kustannustehokkaan, käyttäjäystävällisen, turvallisen ja luotettavan pääsyn. Voi valita yritykselle parhaiten sopivimman hallintaversion Free, Essentials, Advantage- ja Premier -versioiden väliltä. (Editions & Pricing n.d.)

Hinnat ovat yrityskohtaisia Cisco Duolla, mutta yleiset listahinnat on listattu Cisco Duon toimesta heidän kotisivuillaan. Frendylla on käytössään parhain ja hintaluokaltaan kallein Duo Premier -versio, jokaa sisältää Duo Essentials ja Duo Advantage -versioiden sisältävät ominaisuudet. Tällä varmistetaan, että kaikki mahdolliset ominaisuudet, joilla parannetaan yrityksen tietoturvaa, on käytössä sekä on olemassa kaikki tarpeellinen työn toteutusta varten.

7.3.1 Duo Free Edition

Ensimmäinen ja myös ainoa ilmainen lisenssivaihtoehdoista on Free-versio, joka on perustaso, mikä tarjoaa ainoastaan 30 päiväksi pääsyn kokeilemaan monivaiheisen todentamisen perusominaisuuksia. Tämän pystyy aktivoimaan muutamassa minuutissa ja se sisältää perustavanlaatuiset todentamisvaihtoehdot, kuten puhelimeen lähetettävät koodit ja push-ilmoitukset. Voit hallita jopa 10 käyttäjää nauttien yhtenäisistä integraatioista käyttäen täysin ilmaista todentajasovellusta. (Duo Free n.d.)

7.3.2 Duo Essentials/MFA Edition

Essentials-versio on hinnaltaan 3 dollaria per käyttäjä, per kuukausi. Vahva monivaiheinen todentaminen, salasanaton SSO ja luotetun päätepisteen vahvistus sisältyvät muun muassa Essentialsiin, joka on monipuolinen kulunvalvontaratkaisu, joka sopii kaikentyyppisiin yrityksiin. Täysin muokattavissa olevat ja käyttäjäystävälliset monivaiheiset todentamisen ratkaisut, kuten FIDO2-standardin mukaiset ja validoidun Duo Push -toiminnon sisältävät, ovat saatavilla Duo Essentialsin kanssa. Tähän palvelutasoon sisältyy kertakirjautuminen, mikä parantaa käyttökokemusta mahdollistamalla pääsyn moniin sovelluksiin yhdellä tunnistejoukolla. FIDO2-standardiin perustuvat tai Duo Mobilen käyttöä edellyttävät salasanattoman todentamisen ominaisuudet lisäävät turvallisuutta ja helppokäyttöisyyttä. Luotettujen päätepisteiden tarkistaminen varmistaa, että vain päätepisteet, jotka on ennalta hyväksytty voivat käyttää yrityksen resursseja, mikä lisää ylimääräistä suojaustasoa. Hyväksytty verkko ominaisuus mahdollistaa suojattujen verkkojen valinnan, joista käyttäjät voivat kirjautua sisään, ja päätepisteiden näkyvyys auttaa IT-ammattilaisia ymmärtämään paremmin käytössä olevien päätepisteiden tietoturvatasoa. Lisäksi Duo Essentials tarjoaa äärettömän määrän sovellusliittimiä, mikä mahdollistaa sujuvan yhteensopivuuden melkein minkä tahansa sovelluksen kanssa. Käyttäjäryhmäkäytännöt parantavat hallinnon tarkkuutta ja turvallisuuden joustavuutta mahdollistamalla tietoturva- ja kulunvalvontakäytäntöjen mukauttamisen tietyille käyttäjäryhmille. (Duo Essentials n.d.)

7.3.3 Duo Advantage/Access Edition

Advantage-versio on hinnaltaan 6 dollaria per käyttäjä, per kuukausi ja on keskimmäinen vaihtoehto hinnoittelussa. Duo Advantage parantaa organisaation turvallisuutta yhdistämällä monikerroksiset suojaukset huipputeknologioihin, jotka eivät ainoastaan vahvista yleistä turvallisuusasentoa vaan myös lisäävät tehokkuutta sekä järjestelmänvalvojien että loppukäyttäjien kannalta. Duo Advantage laajentaa Duo Essentials -paketin perusominaisuuksia sisällyttämällä siihen riskiperusteisen todentamisen, joka muuttaa suojausasetuksia henkilön tai päätepisteen aiheuttaman vaaran asteen mukaan. Mukautuvat käyttöoikeuskäytännöt mahdollistavat dynaamiset tietoturvamuutokset käyttäjien käyttäytymisestä ja kontekstista riippuen, kun taas päätepisteiden kuntotarkastukset takaavat, että vain organisaation terveyskriteerit täyttäville päätepisteille myönnetään pääsy. Lisäksi koneoppimisen tukema uhkien havaitseminen tarjoaa ennaltaehkäise-

viä vastatoimia uusia tietoturvariskejä vastaan. Viimeisenä Duo Advantage tarjoaa järjestelmänvalvojille perusteellisen ja toimivan kuvan yrityksen tietoturvaympäristöstä täysin toimivien hallintapaneelien ja laajojen raportointiominaisuuksien kautta. (Duo Advantage n.d.)

7.3.4 Duo Premier/Beyond Edition

Premier-versio on hinnaltaan 9 dollaria per käyttäjä, per kuukausi ja on siten kallein vaihtoehto. Yhdistämällä kehittyneitä pääsyratkaisuja Duon vahvaan suojausarkkitehtuuriin luottamuksellisten tietojen ja sovellusten suojaamiseksi Duo Premier parantaa merkittävästi yrityksen turvallisuutta. Kaikki Duo Essentialsin ja Duo Advantagen ominaisuudet sisältyvät tähän premium-pakettiin mukaan lukien kertakirjautuminen, luotetun päätepisteen vahvistus ja monivaiheinen todentaminen FIDO2- ja Duo Verified Push -tuella. Lisäksi se tarjoaa rajattomat sovellusliittimet, salasanattoman todentamisen ja kattavan päätepisteen näkyvyyden. Duo Network Gatewayn tarjoama VPN:stä vapaa etäkäyttö, joka helpottaa suojattujen yhteyksien muodostamista yrityksen resursseihin mistä tahansa erottaa Duo Premierin. Palvelu vahvistaa turvallisuutta entisestään riskiperusteisen todentamisen, perusteellisten päätepisteiden kuntotarkastusten ja koneoppimiseen perustuvan todentamisen havaitsemiin sekä muuttuviin uhkiin reagoivien mukautuvien pääsynvalvontatoimintojen avulla. Laajat hallintapaneelit ja raportointityökalut tarjoavat syvällisiä näkemyksiä organisaation turvallisuustilanteesta, ja päätepisteiden suojaustarkistukset ja VPN:stä vapaa suojattu etäkäyttö takaavat, että vain yhteensopivat päätepisteet voivat muodostaa yhteyden noudattaen tiukkoja turvallisuusstandardeja käyttäjän mukavuudesta tai tuottavuudesta tinkimättä. (Duo Premier n.d.)

8 Toteutuksen asennus

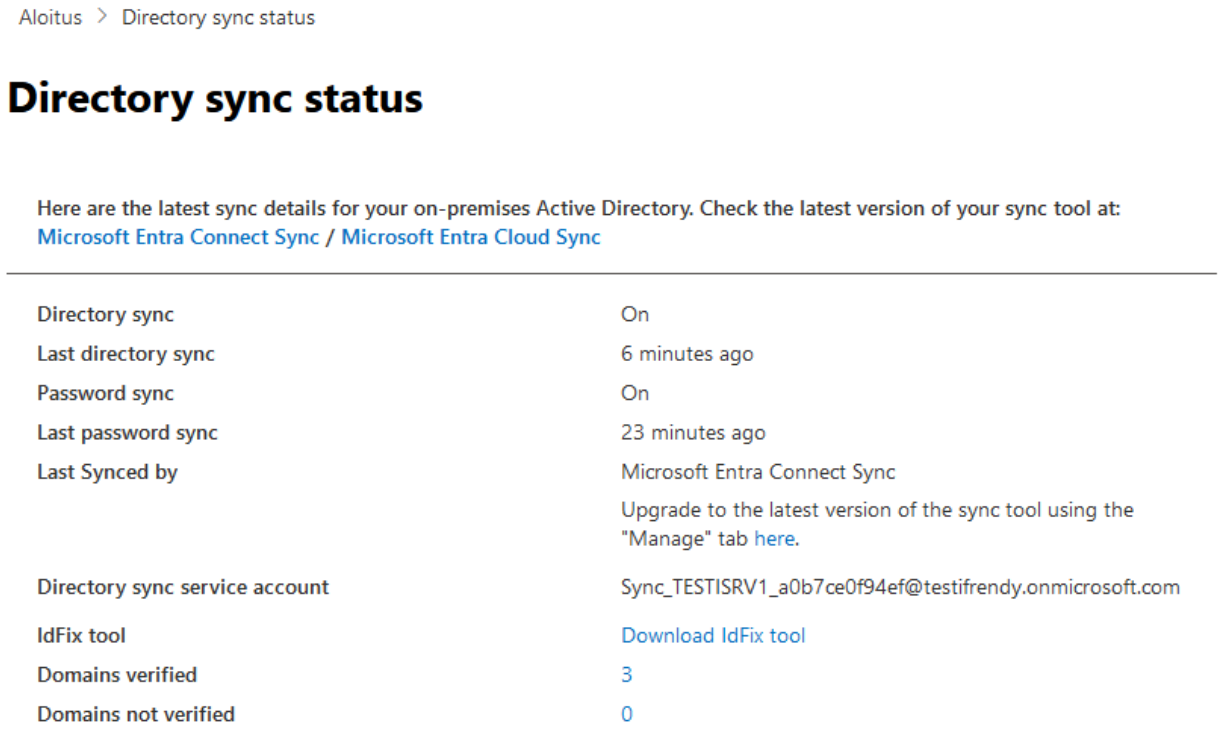
Toteutuksen asennusvaiheessa pidettiin yhteyttä toimeksiantajan tietoturvapuolen asiantuntijoiden kanssa tietyin väliajoin palaverien ja keskustelujen muodossa etenkin ongelmatilanteissa sekä lisäksi tarkasteltiin käyttöönoton sen hetkistä tilaa, esiin nousseita kysymyksiä. Tätä käytäntöä toteutettiin toteutuksen aikana ja aina tarpeen tullessa kontaktoitiin toimeksiantajan asiantuntijoita sekä pidettiin heidät tietoisena käyttöönoton kehityksestä. Projektin toteutuksen aikana oli kuitenkin paljon itsenäistä tutkimistyötä sekä testausta ja asioita enemmän varmisteltiin vain asiantuntijoiden kanssa. Tämä oli toisaalta todella hyvä asia oppimisen kannalta, koska aiheeseen piti todella itse perehtyä ja sai oppia muun muassa erehdysten kautta. Toteutusta varten projektille ei ollut

varsinaista paikkaa, johon raportoitiin mitä oli tehty, vaan kaikki otettiin talteen valmiiksi tähän opinnäytetyön pohjaan, josta ne muokattiin valmiiksi.

Tämän osion kappaleissa käsitellään Cisco Duo MFA:n asennusprosessia alusta alkaen Frendyn testiympäristössä. Asennus alkoi MFA:n konfiguroinnilla ja integroinnilla olemassa olevaan IT-infrastruktuuriin mukaan lukien Microsoft Active Directory ja Microsoft Entra ID palveluineen. Keskeisiä askeleita olivat käyttäjätietojen synkronointi ja Duo MFA -sovelluksen asennus ja testaus käyttäjän päätepisteellä. Käyttöönottoon liittyi myös Duo MFA:n mukauttaminen organisaation erityistarpeisiin, kuten käyttäjien sijainnin ja laitetyypin huomioiminen. Lisäksi tarkasteltiin asennuksen onnistumista, haasteita ja niiden ratkaisuja sekä arvioitiin asennusprosessin vaikutuksia organisaation tietoturvaan ja käyttäjäkokemukseen.

8.1 Microsoft Entra Connect synkronointi

Microsoft Active Directoryn ja Microsoft Entra ID:n synkronointi on keskeinen osa IT-infrastruktuurin hallintaa ja käyttäjätietojen yhdenmukaistamista. Synkronoinnin avulla organisaation sisäiset käyttäjätunnukset ja pääsyoikeudet heijastuvat suoraan Microsoft Entra ID:n pilvipalveluihin, mikä mahdollistaa identiteettien yhtenäisen hallinnan sekä paikallisissa että pilvipohjaisissa ympäristöissä. Tämä synkronointi mahdollistaa yksinkertaisen ja turvallisen SSO-kokemuksen käyttäjille parantaen samalla tietoturvaa ja alentaen käyttökatkosten riskiä. Lisäksi synkronointi helpottaa uusien käyttäjien lisäämistä ja olemassa olevien käyttäjätietojen päivittämistä, kun muutokset paikallisessa AD:ssa päivittyvät automaattisesti Microsoft Entra ID:seen. Tämä integraatio on elintärkeä organisaation kyvylle ylläpitää ajantasaisia käyttäjäprofiileja ja hallita pääsyoikeuksia tehokkaasti niin paikallisten resurssien kuin pilvipalveluiden osalta. Kuviossa 12 näkyvän Microsoft 365 admin centerin hakemiston synkronointi tilan kautta nähdään, milloin viimeksi hakemisto- ja salasana -synkronoinnit ovat menneet lävitse sekä lisäksi pystytään varmistamaan minkä nimiseltä palvelimelta synkronointi tapahtuu. Lisäksi samasta kohdasta nähdään, jos synkronoinnissa on ollut virheitä tai se on epäonnistunut kokonaan.

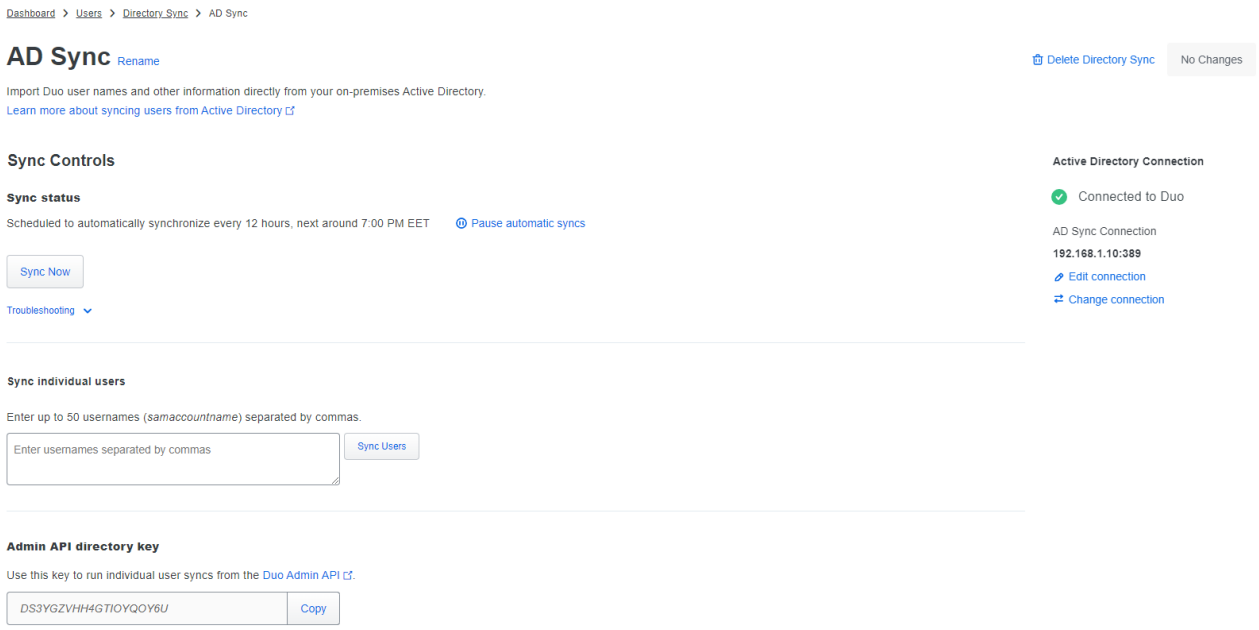


Kuvio 12. Hakemiston synkronoinnin tila Microsoft 365 admin centerissä

Lisäksi testiympäristössä on AD:lta suoraan synkronointi Cisco Duoon, jota voidaan tarkastella Duon hallintapaneelissa Duo Sync -kohdassa, jossa testiympäristön Microsoft Active Directory -käyttäjätiedot synkronoidaan Duon hallintapaneeliin näkyviin. Tämä mahdollistaa käyttäjähallinnan keskitetyn hallinnan, helpottaa käyttöoikeuksien hallintaa ja varmistaa, että käyttäjätiedot ovat johdonmukaisia koko organisaatiossa.

Tämän Duo Sync -toiminnon avulla voit tuoda Duon järjestelmänvalvojat tai loppukäyttäjät suoraan AD LDS -esiintymästä tai paikallisesta AD-metsästä tai -alueesta. Tietoja ei ole tuotu takaisin käyttäjähakemistoosi Duosta, koska tämä synkronointi on yksisuuntainen. Koko hakemisto synkronoidaan kahdesti päivässä aikataulun mukaisesti täydellisen käyttäjien hallinnan varmistamiseksi. Järjestelmänvalvojien synkronointi tapahtuu puolen tunnin välein. Lisäksi voi aloittaa kumman tahansa täydellisen synkronoinnin milloin tahansa suoraan Duon hallintapaneelista. Yksittäisten käyttäjien tai järjestelmänvalvojien synkronoinnit voidaan suorittaa myös ohjelmallisesti käyttämällä Admin API:ta tai pyynnöstä hallintapaneelista tarkempien päivitysten saamiseksi. (Active Directory Sync for Duo Users and Admins 2023.)

Kohdennettiin synkronointi siten, että tuotiin synkronoinnissa AD:lta vain Duo-sync -ryhmään kuuluvat käyttäjät, jolla varmistettiin AD:lta tulevan vain tarpeelliset käyttäjät. Konfiguroitiin Duon hallintapaneelissa kuviossa 13 nähtävään AD synkronoinnin asetuksiin integrointiavain, salainen avain sekä API isäntänimi sen jälkeen, kun oli asennettu Duon todennusvälityspalvelin TESTISRV1-palvelimelle. Ladattiin esikonfigurointi tiedosto palvelimelta, josta saatiin nämä tarvittavat tiedot. Asetettiin TESTISRV1-palvelimen IP-osoite portteineen toimialueen ohjain -kohtaan ja pohja DN, jossa synkronointiin halutut käyttäjät sijaitsivat palvelimen AD:lla.



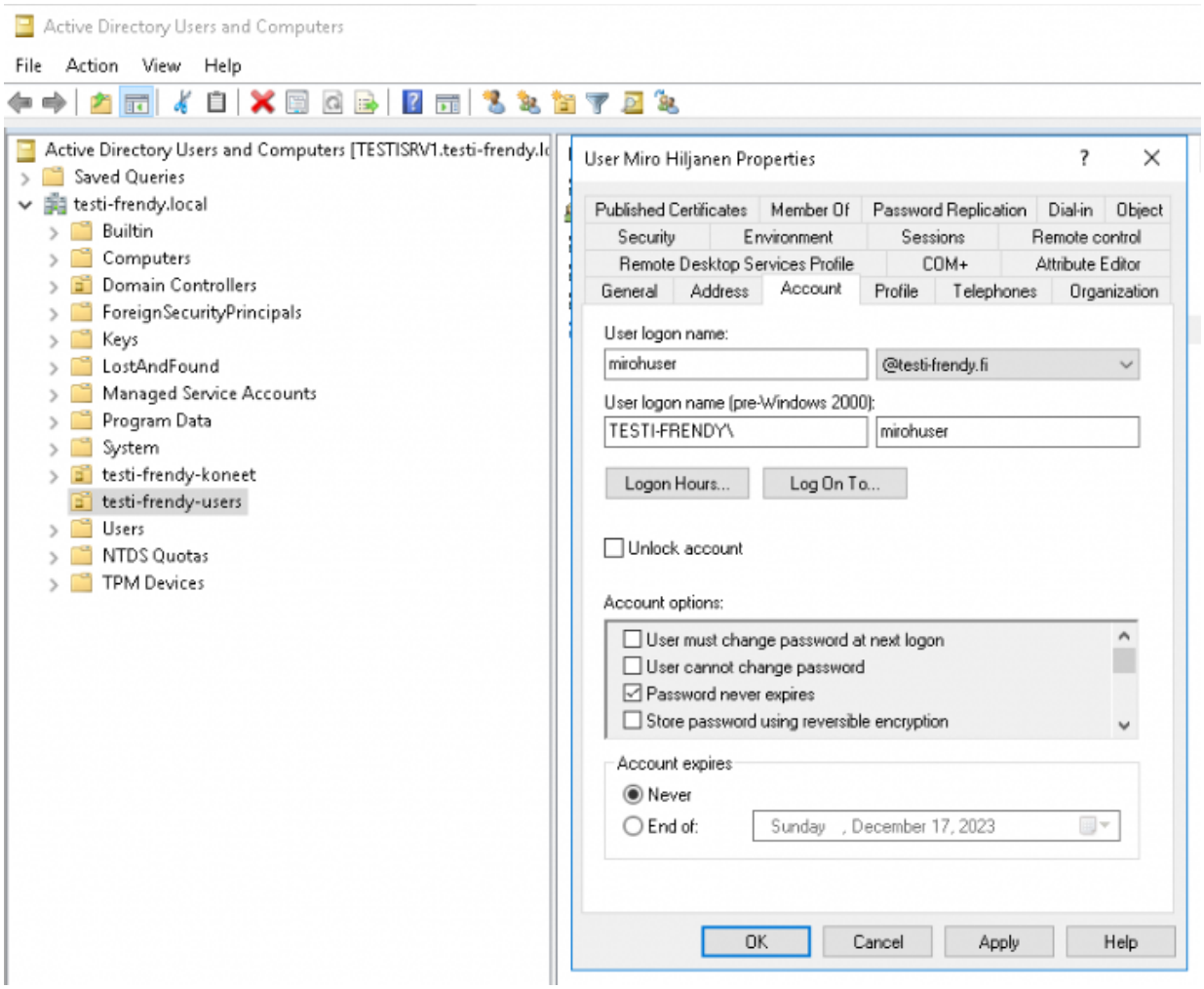
Kuvio 13. AD synkronointi Cisco Duossa

8.2 Käyttäjätunnusten luonti Microsoft Active Directoryssa ja Microsoft 365 -lisenssien allokointi

Olennainen hakemistopalvelu nimeltä Active Directory Domain Services luo hierarkkisen rakenteen verkko-objekteja koskevien tietojen tallentamiseen ja hallintaan mukaan lukien käyttäjätilit puhelinnumeroineen, salasanoineen ja nimineen, jotta järjestelmänvalvojat sekä valtuutetut käyttäjät voivat käyttää sitä. AD DS:n perusta on jäsennelty tietovarasto, jossa yhdistyvät tietoturvaominaisuudet kuten kirjautumisen todentaminen ja hakemistokohteiden pääsynhallinta. Se tarjoaa loogisen ja hierarkkisen hakemistotietojen rakenteen. Tämän ansiosta käyttäjät voivat käyttää tarvittavia resursseja tehokkaasti kaikkialla verkossa ja järjestelmänvalvojat voivat hallita verkkoresursseja yhdellä kirjautumisella. Maailmanlaajuinen luettelo, joka tarjoaa yksityiskohtaisia tietoja

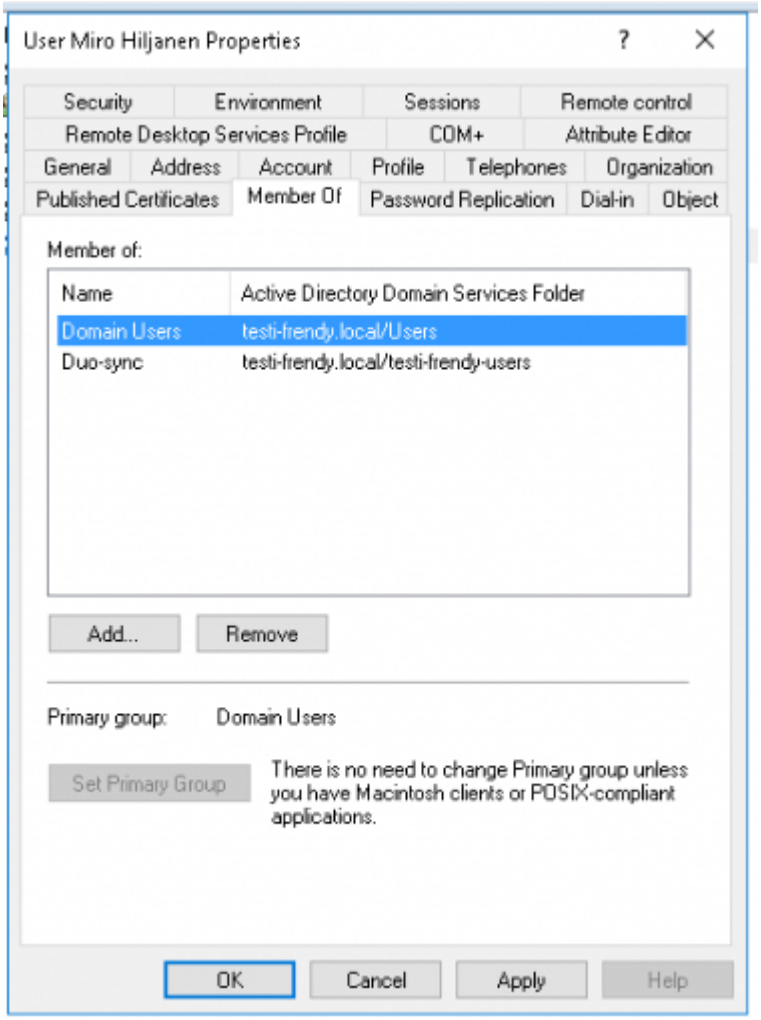
jokaisesta objektista yksinkertaista tiedonhakua varten, kysely- ja indeksimekanismin objektien löytämiseen, replikointipalvelu, joka ylläpitää hakemistotietojen yhdenmukaisuutta toimialueen kaikissa toimialueen ohjauskoneissa sekä skeeman, joka määrittää objektien ja attribuuttien luokat. Hakemistossa on kaikki Active Directoryn lisäominaisuudet, jotka mahdollistavat vankan ja käytäntöihin perustuvan hallinnan jopa monimutkaisissa verkkoympäristöissä. (Active Directory Domain Services Overview 2022.)

Luotiin käyttäjä ympäristön TESTSRV1-palvelimelle Active Directory -ohjaimelle testaamista varten ja, jolle saatiin myöhemmin pakotettua Cisco Duon monivaiheinen todentaminen käyttöön. Toiminnan kannalta oli tärkeää, että käyttäjä luotiin @testi-frendy.fi -sähköpostin päätteellä ja testi-frendy-users OU:n alle, jotta se synkronoituu oikein Microsoft Entran puolelle. Kuviossa 14 nähdään käyttäjän tiliasetukset ja käyttäjä oikeassa OU:ssa.



Kuvio 14. Käyttäjän ominaisuudet Active Directorylla

Lisättiin käyttäjä AD:lla jo valmiiksi luotuun Duo sync -ryhmään, joka oli määritetty Duon hallinta-paneelissa ryhmäksi, minkä kautta käyttäjä siirtyi Active Directory synkronoinnin avulla myös Cisco Duon puolelle. Kuviossa 15 näytetään käyttäjän ryhmäjäsenyydet.



Kuvio 15. Käyttäjän ryhmäjäsenyydet Active Directorylla

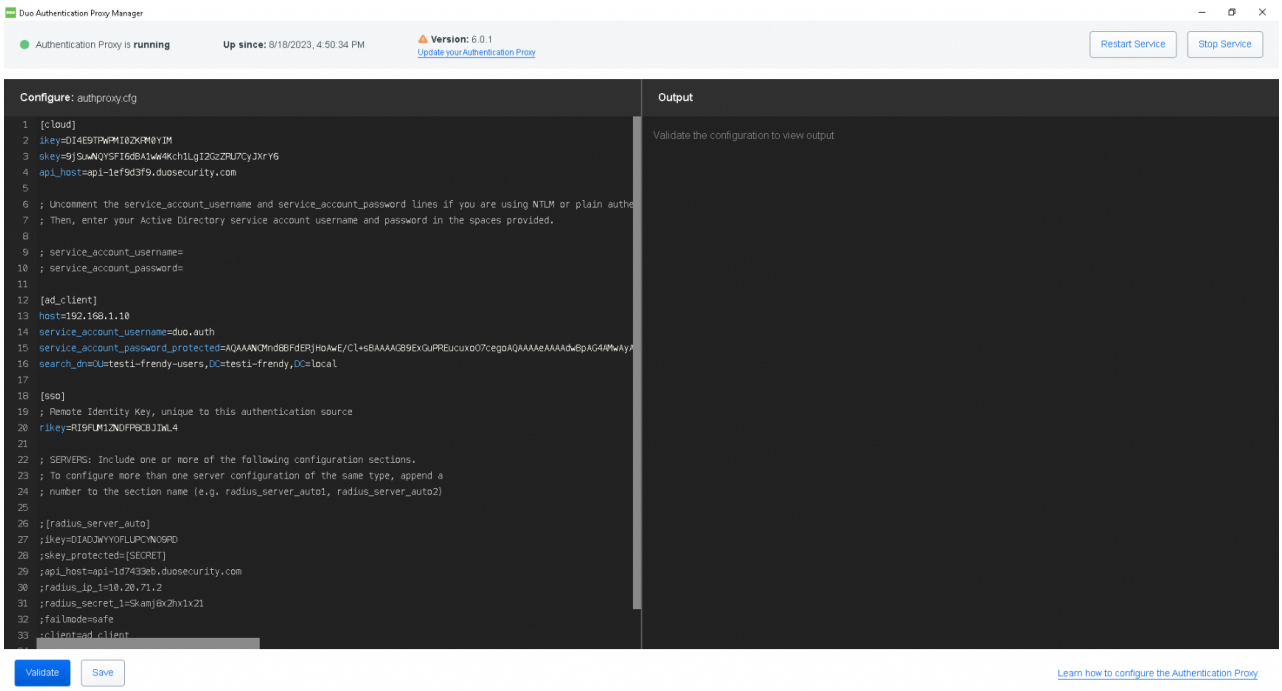
Varmistettiin, että synkronointi meni läpi myös Active Directorylta Microsoft Entra ID:n puolelle ja kohdistettiin tässä tapauksessa tarvittava Microsoft 365 Business Premium -lisenssi käyttäjälle käyttöön.

8.3 Duo Authentication Proxy määritys

Paikallinen ohjelmistopalvelu nimeltään Duo Authentication Proxy käsittelee todentamispyyntöjä paikallisista päätepisteistä ja sovelluksista LDAP:n tai RADIUS:n avulla. Se voi käyttää jo olemassa

olevaa RADIUS-palvelinta tai LDAP-hakemistoa ensisijaiseen todentamiseen, ja siten se voi käyttää Duoa toissijaiseen todentamiseen. Tämä Duon todennusvälityspalvelin myöntää pääsyn päätepisteeseen tai sovellukseen, kun käyttäjä vahvistaa kaksivaiheisen todentamispyynnön. Duo Authentication Proxy Manager -niminen Windows-työkalu auttaa Duo Authentication Proxy -palvelimen asetusten muuttamisessa, välityspalvelimen tilan tarkistamisessa sekä todennusvälityspalvelin palvelun käynnistämisessä ja lopettamisessa. (Duo Authentication Proxy – Reference 2023.)

TESTISRV1-palvelimelle oli valmiiksi asennettuna Duo Authentication Proxy Manager -ohjelma ja kuviossa 16 nähdään sen olevan määritetty oikein, jotta se oli yhdistettynä Cisco Duoon onnistuneesti.

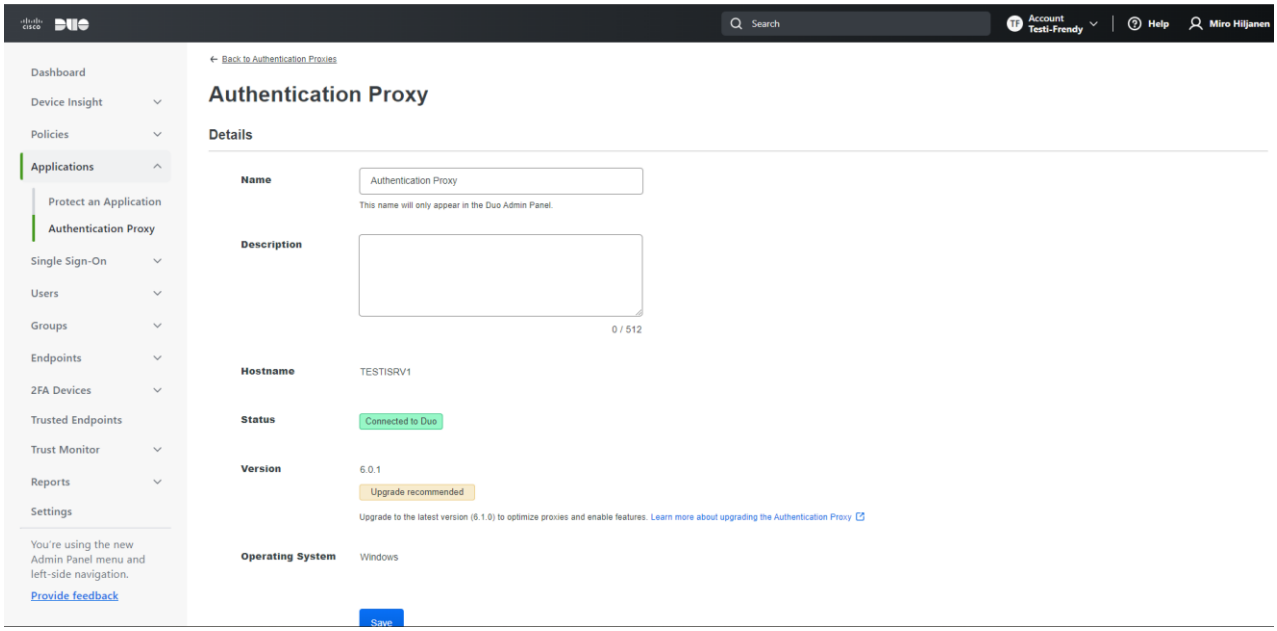


Kuvio 16. Duo Authentication Proxy Manager konfiguraatio

Duo Authentication Proxy -palvelimen authproxy.cfg-määritystiedosto löytyy välityspalvelimen asennushakemiston conf-alikansiosta. Tiedosto on rakenteeltaan kuten INI-tiedosto, jossa ”nimi=arvo” -parit edustavat asetusvaihtoehtoja ja hakasulkeet erottavat osia. Active Directory- tai LDAP-pohjaisen ensisijaisen todentamisen määrittäminen edellyttää sellaisten osien käyttöä, kuten ”[ad_client]”, jotka sisältävät tietoja toimialueen ohjaimen osoitteesta, palvelutilin tunnistetie-

doista ja hakupohjan DN:stä käyttäjien hakuja varten. ”REM”, ”#” tai ”;” voidaan lisätä kommentteja asetustiedostoon, mikä on hyödyllistä osien selkeässä merkitsemisessä. Tämä tiedosto määrittää myös lokin asetukset ja virheenkorjausvaihtoehdot, mikä mahdollistaa laajan toiminnallisen lokikirjauksen vianmääritystä varten. (Duo Authentication Proxy – Reference 2023.)

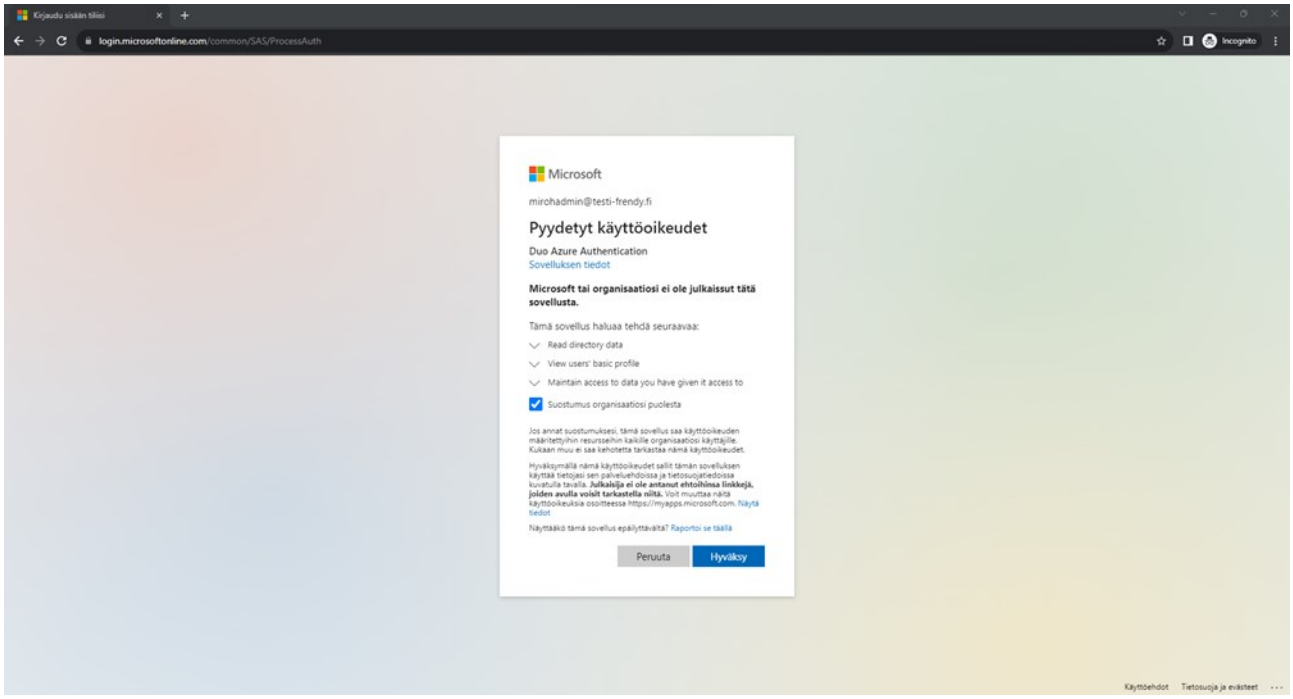
Duon hallintapaneelin kautta sovellusten alta myös nähdään kuviossa 17, että Authentication Proxy on yhdistettynä TESTISRV1-palvelimelle. Todentamisen lähteissä oli aktiivisena ympäristön Active Directory, joka käytti SSS-todentamiseen äsken tarkasteltua Authentication Proxya.



Kuvio 17. Authentication Proxy Duossa

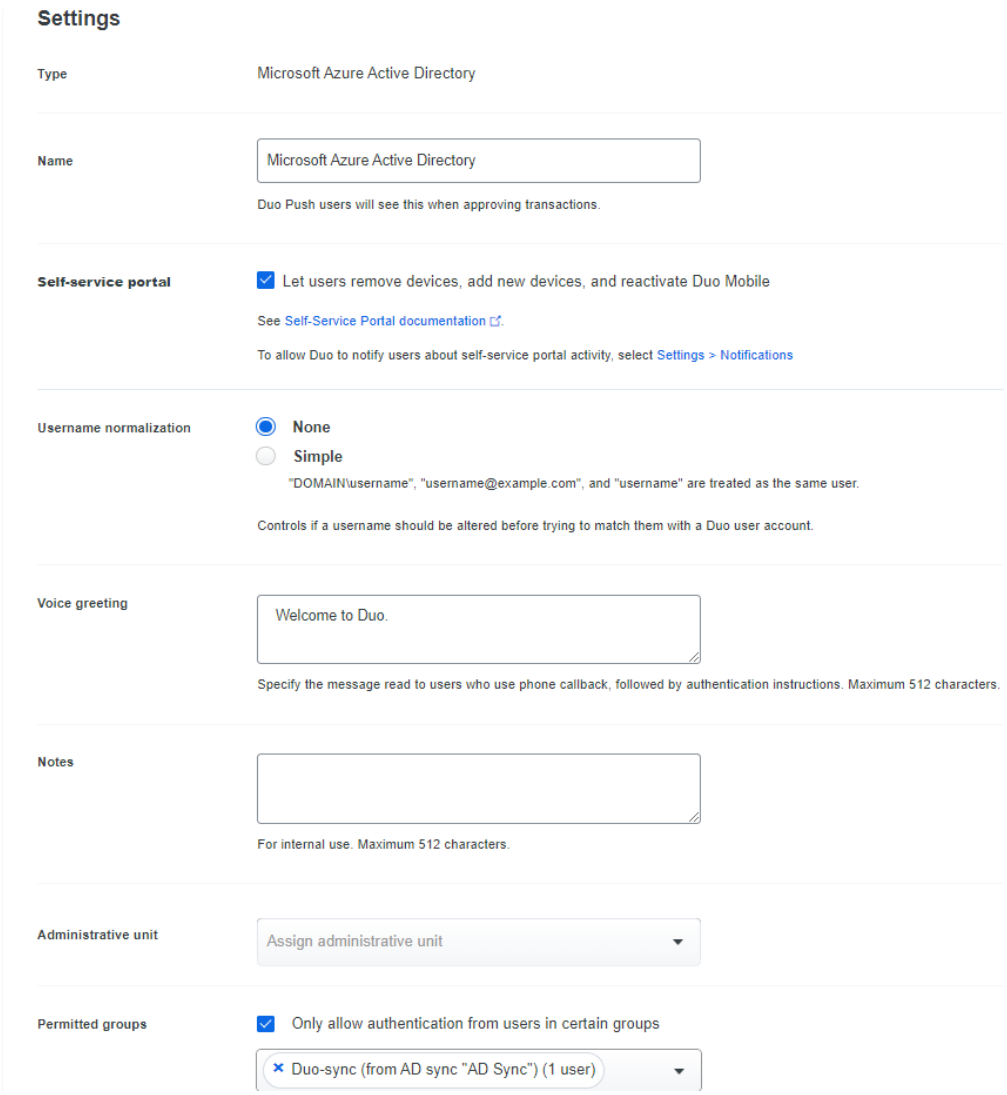
8.4 Microsoft Azure Active Directory -sovelluksen suojaus Duossa

Aloitettiin suojaamalla uusi sovellus hakemalla Duon sovelluskirjastosta vielä vanhalla nimellä Microsoft Azure Active Directory, joka nykyään tunnetaan nimellä Microsoft Entra ID. Tämän jälkeen valtuutettiin Duolle lukuoikeudet testiympäristön Microsoft Entra -vuokralaiselle napsauttamalla valtuuta ja jatkettiin eteenpäin. Kirjauduttiin sisään vuokralaiseen järjestelmänvalvojatilillä ja kuviossa 18 nähdään, kun annettiin suostumus organisaation puolesta hyväksymällä tarvittavat lukuoikeudet Microsoft Entra ID:seen, jotta Duo pystyi käyttämään ja lukemaan Microsoft Entra -vuokralaiselta tietoja.



Kuvio 18. Duo Azure Authentication -käyttöoikeuksien hyväksyntä

Käyttöoikeuspyynnön hyväksymisen jälkeen palattiin sovelluksen asetussivulle, josta kopioitiin JSON-teksti talteen. Annettiin olla oletuksena kaikki asetukset lukuun ottamatta kuviossa 19 näkyvää sallitut ryhmät -kohtaa, johon asetettiin aiemmin luotu Duo-sync -ryhmä TESTISRV1-palvelimen AD:lta.



Kuvio 19. Microsoft Azure Active Directory -sovelluksen asetukset Duossa

8.5 Microsoft Entran ehdollisen pääsyn konfigurointi Duoon

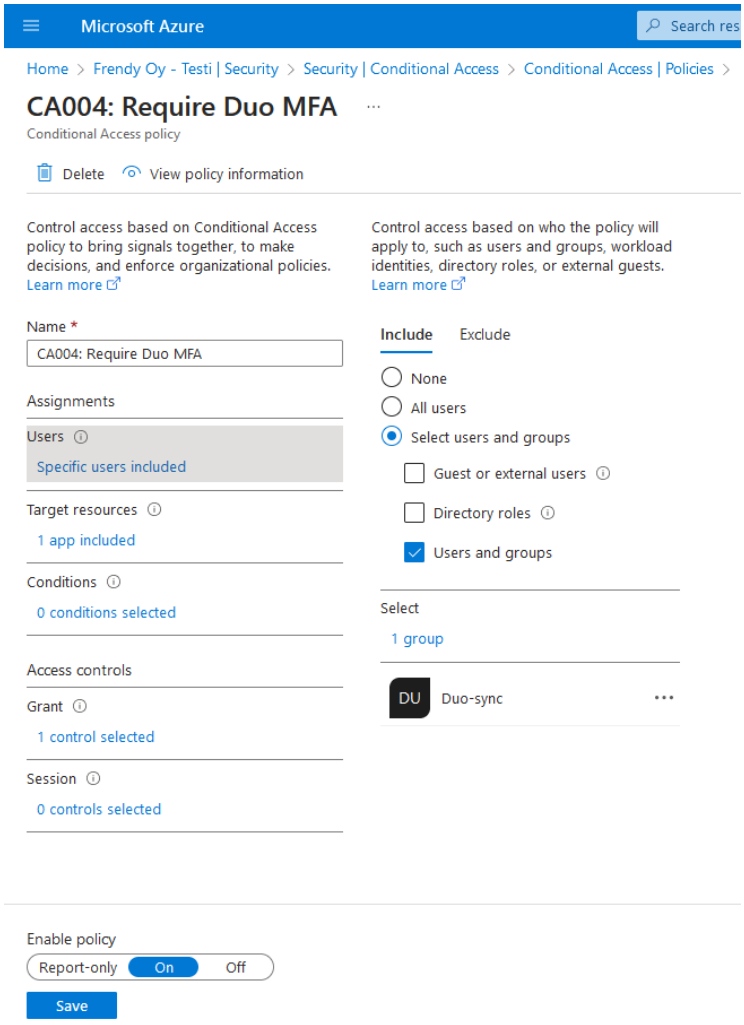
Ehdollinen pääsy on ominaisuus, jota Microsoft Entra käyttää määrittämään käytäntöjä, jotka ohjaavat sovellusten käyttöä tiettyjen vaatimusten, kuten käyttäjäryhmän jäsenyyden tai maantieteellisen sijainnin perusteella. Duo voi tarjota vahvan kaksivaiheisen todentamisen käyttäjien kirjautumisille integroimalla Microsoft Entra CA:n. Asennuksen onnistumiseksi on luotava vanhalla nimellä oleva Microsoft Azure CA -sovellus Duon hallintapaneeliin, valtuutettava käyttämään Microsoft Entra -vuokraajaa ja määritettävä vaadituilla oikeuksilla sekä asetuksilla. Ennen kuin määritetään Duon todentaminen, niin on varmistettava, että on aktiivinen Microsoft Entra ID P1- tai P2-tilaus ja valittu järjestelmänvalvojan palvelutili, jolla on maailmanlaajuiset järjestelmänvalvojan

ominaisuudet. (Duo Two-Factor Authentication for Microsoft Entra ID (formerly Azure Active Directory) 2023.)

Määritettiin uusi mukautettu ohjausobjekti Microsoft Entra ID:ssä ja nimettiin se ”RequireDuoMFA”. Kuviossa 20 nähdään, että liitettiin mukautetun ohjausobjektin JSON-tekstiin aiemmin Duo hallintapaneelista Microsoft Azure Active Directory -sovellussivulta kopioitu JSON-teksti ja luotiin ohjausobjekti valmiiksi.

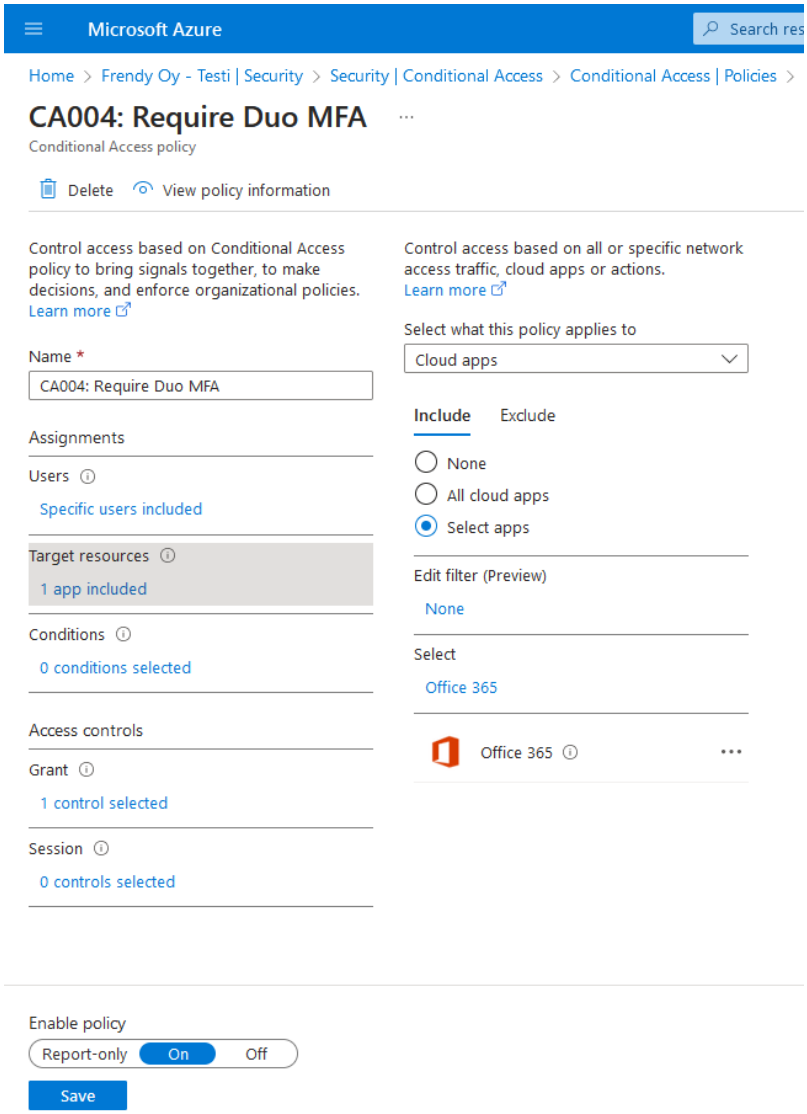
Kuvio 20. Microsoft Entra CA:n mukautetut säätimet -lisäasetukset

Luotiin seuraavaksi ehdolliseen pääsyyn käytäntö nimeltään ”Require Duo MFA” ja käyttäjät-kohdassa kohdennettiin se pelkästään Duo-sync -ryhmälle, mitkä näkyvät kuviossa 21.



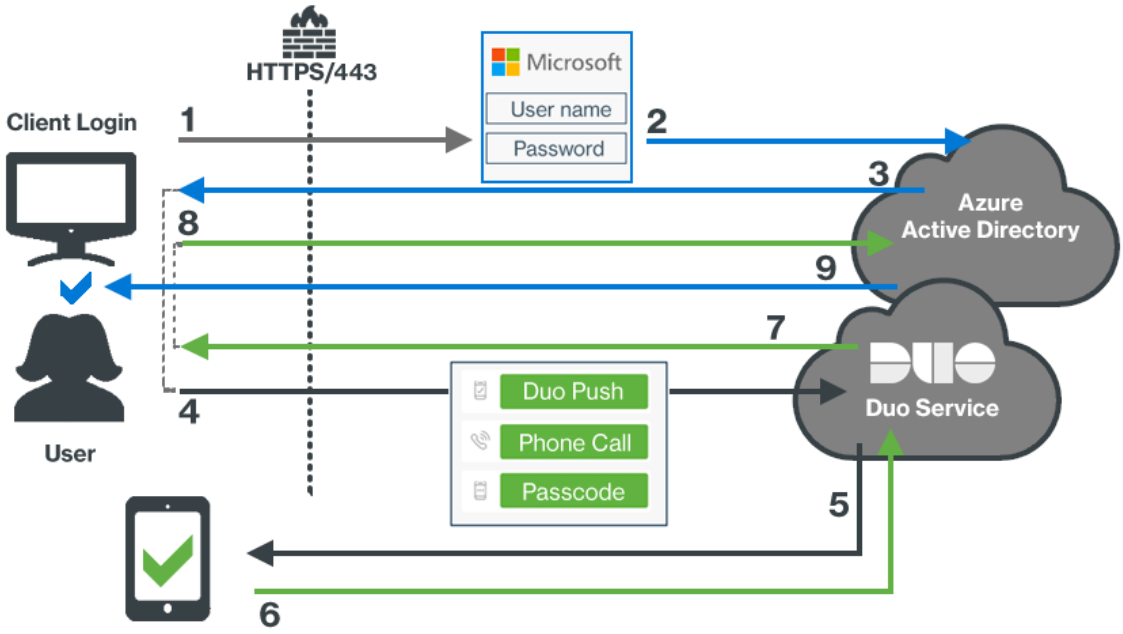
Kuvio 21. Microsoft Entra CA:n käytännön käyttäjät

Kuviossa 22 nähdään, että valikoitiin käytännön kohderesurssiksi Office 365 -sovellus kokonaisuudessaan, jotta saatiin Duo MFA vaadittua käyttäjille heti, kun he yrittivät kirjautua mihin vain Office 365 -sovelluksiin.



Kuvio 22. Microsoft Entra CA:n käytännön kohderesurssit

Myönnettiin käytännön käyttöoikeuksista pääsy käyttäen luotua mukautettua RequireDuoMFA ohjausobjektia. Asetettiin käytäntö päälle ja luotiin käytäntö valmiiksi. Voitiin todeta määritysten lopuksi, että kirjautuminen Office 365:een testiympäristön Duo-sync -ryhmään kuuluvilla käyttäjillä noudatti onnistuneesti kuviossa 23 nähtävää Microsoft Entran ehdollisen pääsyn kaaviota.



Kuvio 23. Duon monivaiheisen todentamisen kaavio Microsoft Entra ID:lle (Duo Two-Factor Authentication for Microsoft Entra ID (formerly Azure Active Directory) 2023)

8.6 Duo Self-Service Portal ja Duo Mobile määritykset

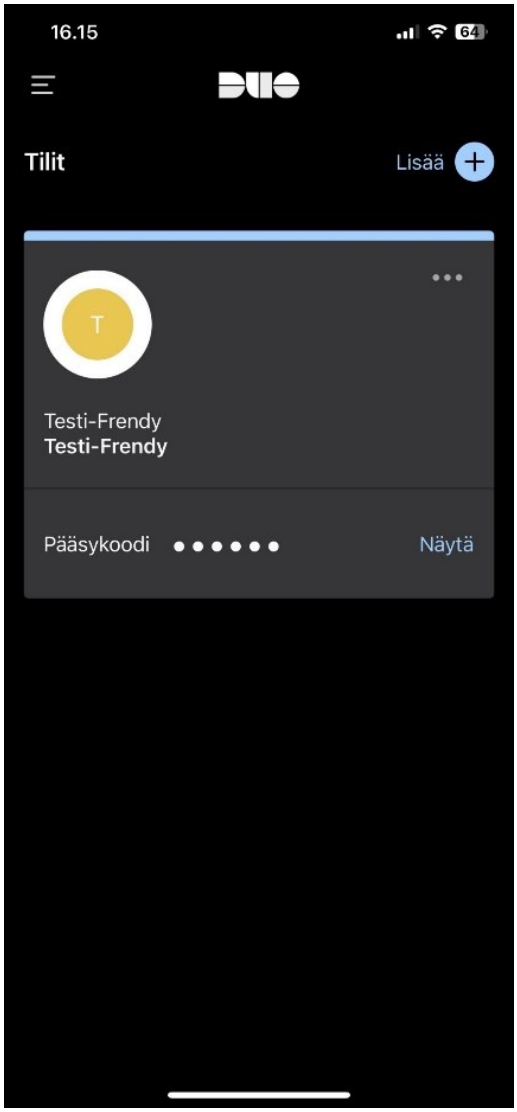
Duo Premier-, Duo Advantage- ja Duo Essentials -pakettien asiakkaat voivat käyttää Duo Device -hallintaportaalia, joka tarjoaa erillisen päätepisteen hallintaliittymän. Tämän sivuston kautta uudet käyttäjät voivat rekisteröidä ensimmäisen todentamislaitteensa, ja nykyiset käyttäjät voivat lisätä, poistaa tai muokata laitteita itse ja nämä kaikki ilman IT-ammattilaisten apua. Portaalin käyttöönotto edellyttää paikallista verkkopalvelinta, jossa on ensisijainen todentaminen käyttäjähakemistoosi, kuten AD tai OpenLDAP. Duo v2 Web SDK:n avulla integrointi edellyttää Duo Device Management Portalin lisäämistä verkkosivustollesi. Tämä edellyttää toisen kirjautumissivun luomista Duon todentamista varten. Käyttäjät pääsevät päätepisteen hallintaportaaliin suoritettuaan onnistuneesti sekä päätodentamisen että Duon vaatiman kaksivaiheisen todentamisen. (Duo Device Management Portal for End Users 2023.)

Kirjauduttiin onnistuneesti Duo itsepalveluportaaliin käyttäen Microsoft Entran ehdollista pääsyä, jonka jälkeen Cisco Duo oletuksena pyytää valikoimaan vaihtoehdon, jota käytetään jatkossa kirjautumiseen. Windows Hello kirjautumisvaihtoehdon valikoimisen jälkeen varmistettiin Windowsin suojauksen PIN-koodilla henkilöllisyys Windows Helloon. Windows Hello oli saatu

lisättyä kirjautumisvaihtoehtoihin ja jatkossa Duolla voitiin kirjautua suoraan käyttämällä päätepisteen Windows Hello -ominaisuutta. Vahvistettiin lisäys todentamalla tekstiviestillä saadulla pääsykoodilla, joka tuli puhelimeen, mikä syötettiin avautuneeseen ikkunaan.

Vielä tässä vaiheessa Duo pyysi lataamaan oletuksena kaikille päätepisteille Duo Device Health -sovelluksen, koska käytäntöjä ei ollut sen osalta säädetty, mutta se ei ollut pakollinen ja se pystyttiin halutessaan ohittamaan. Duo Device Health, joka tunnetaan nykyään myös Duo Desktop nimellä, tarkisti päätepisteen suojauksen siten, että se tarkisti Windowsin olevan ajan tasalla, järjestelmän salasanan olevan asetettu, BitLockerin olevan käytössä ja palomuurin olevan käytössä. Päätepiste läpäisi kaikki nämä tarkastukset, joten voitiin jatkaa Duo Mobilen määritykseen, joka oli Duon suositeltu vaihtoehto kirjautumiseen. Myöhemmin tarkastellaan tarkemmin Duo Desktopin tarkistuksia ja toimintaa.

Annettiin puhelinnumero Duo Mobilea varten ja asennettiin tämä Duo Mobile -sovellus sovelluskaupasta puhelimeen. Avattiin se puhelimella ja aloitettiin tilin lisääminen oikean yläkulman Lisää-kohdasta. Valikoitiin käyttämään QR-koodia, koska se oli varma ja toimi parhaiten tilien lisäämiseen, jonka jälkeen skannattiin päätepisteen ruudulla näkyvä koodi. Varmistettiin, että tilin lisääminen Duo Mobileen onnistui ja kuviossa 24 nähdään tili sovelluksessa sisältäen myös pääsykoodin, jos sitä haluttiin käyttää kirjautumisessa. Duo Mobile oli nyt lisätty ja sitä voitiin käyttää kirjautumiseen käyttämällä siihen lähetettäviä push-ilmoituksia. Lisäksi pystyttiin käyttämään toissijaisesti tekstiviestejä ja puheluita, joita voitiin vastaanottaa puhelinnumeroon, joka oli aiemmin annettu.

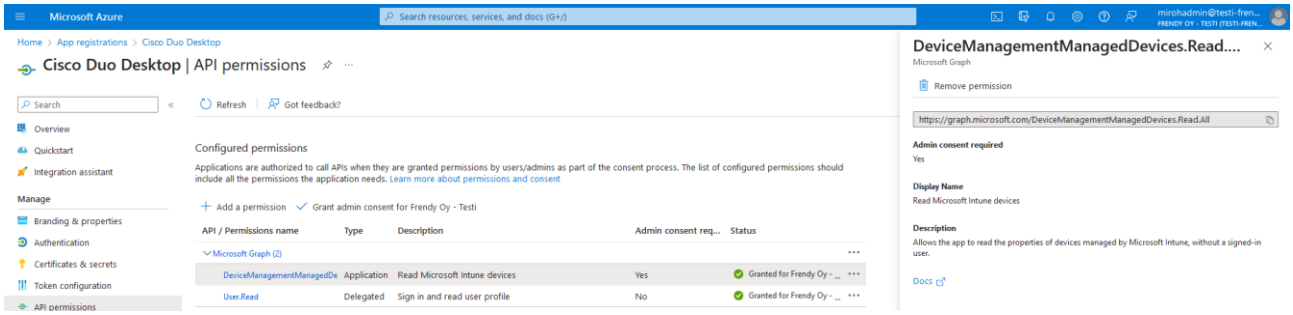


Kuvio 24. Duo Mobile -sovellus iOS-laitteessa

8.7 Duo Trusted Endpoints -käytännön ja Intune with Duo Desktop -integraation määritys

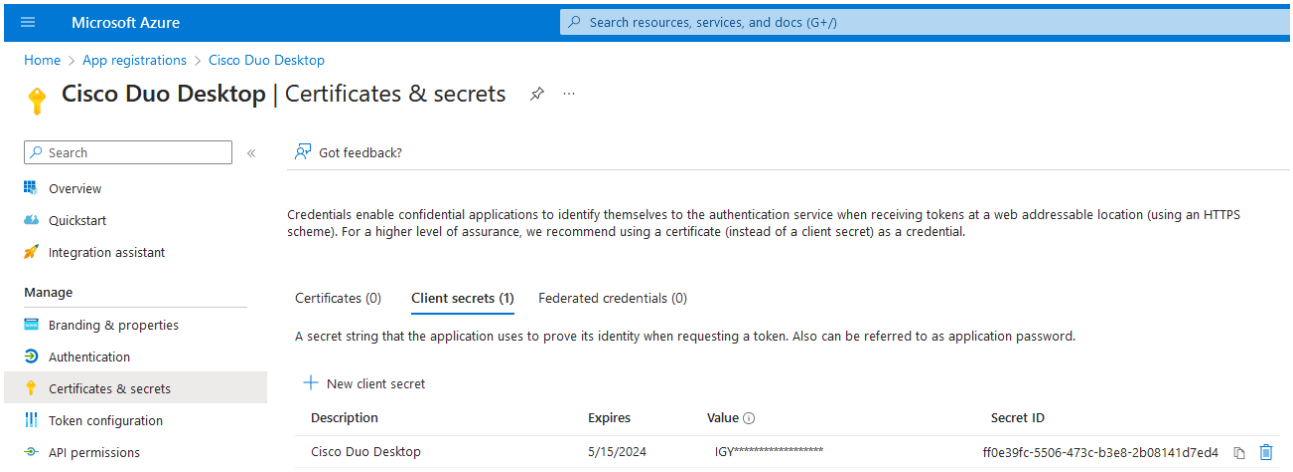
Duon Trusted Endpoints -käytäntö voidaan määrittää Windows-ympäristöihin käyttämällä Intune with Duo Desktop -integraatiota. Tämä asetus varmistaa, että vain Intunen hallinnoimat ja organisaatiosi suojausstandardit täyttävät päätepisteet voivat käyttää Duon suojaamia sovelluksia. Määritysprosessiin kuuluu Duolle ominaisen Microsoft Azure Active Directory -sovelluksen määrittäminen, sen rekisteröiminen Duoon ja tämän asennuksen integrointi Intune-hallintaan päätepisteen yhteensopivuuden hallintaa ja tarkistamista varten. Tämä integrointi vahvistaa turvallisuutta sallimalla vain luotettujen ja varmennettujen päätepisteiden pääsyn kriittisiin sovelluksiin ja tietoihin, mikä noudattaa vankkoja käyttöoikeuksien hallintakäytäntöjä. (Duo Trusted Endpoints 2023.)

Lisättiin Intune with Duo Desktop Duon hallintapaneelissa saatavilla olevista Trusted Endpoints hallintatyökalujen integroinneista. Avattiin lisätty integraatio ja se sisälsi 4 eri asennuksen vaihetta. Luotiin Microsoft Azure Active Directory -sovellus kirjautumalla Microsoft Azure -konsoliin järjestelmänvalvojatilillä. Valittiin verkkotunnus ja siirryttiin sitten Hallinnoi-osion kohtaan Sovellusten rekisteröinnit. Luotiin uusi rekisteröinti, annettiin sovellukselle kuvaava nimi ja asetettiin "Vain tämän organisaatiohakemiston tilit" tuetuksi tilityypiksi. Kuviossa 25 nähdään, kun rekisteröinnin jälkeen lisättiin API-oikeudet valitsemalla Microsoft Graph ja erityislupa "DeviceManagementManagedDevices.Read.All" kohdasta Application Permissions. Annettiin lopuksi järjestelmänvalvojan suostumus kaikille Azure-verkkotunnuksen tileille suorittaakseen prosessin loppuun.



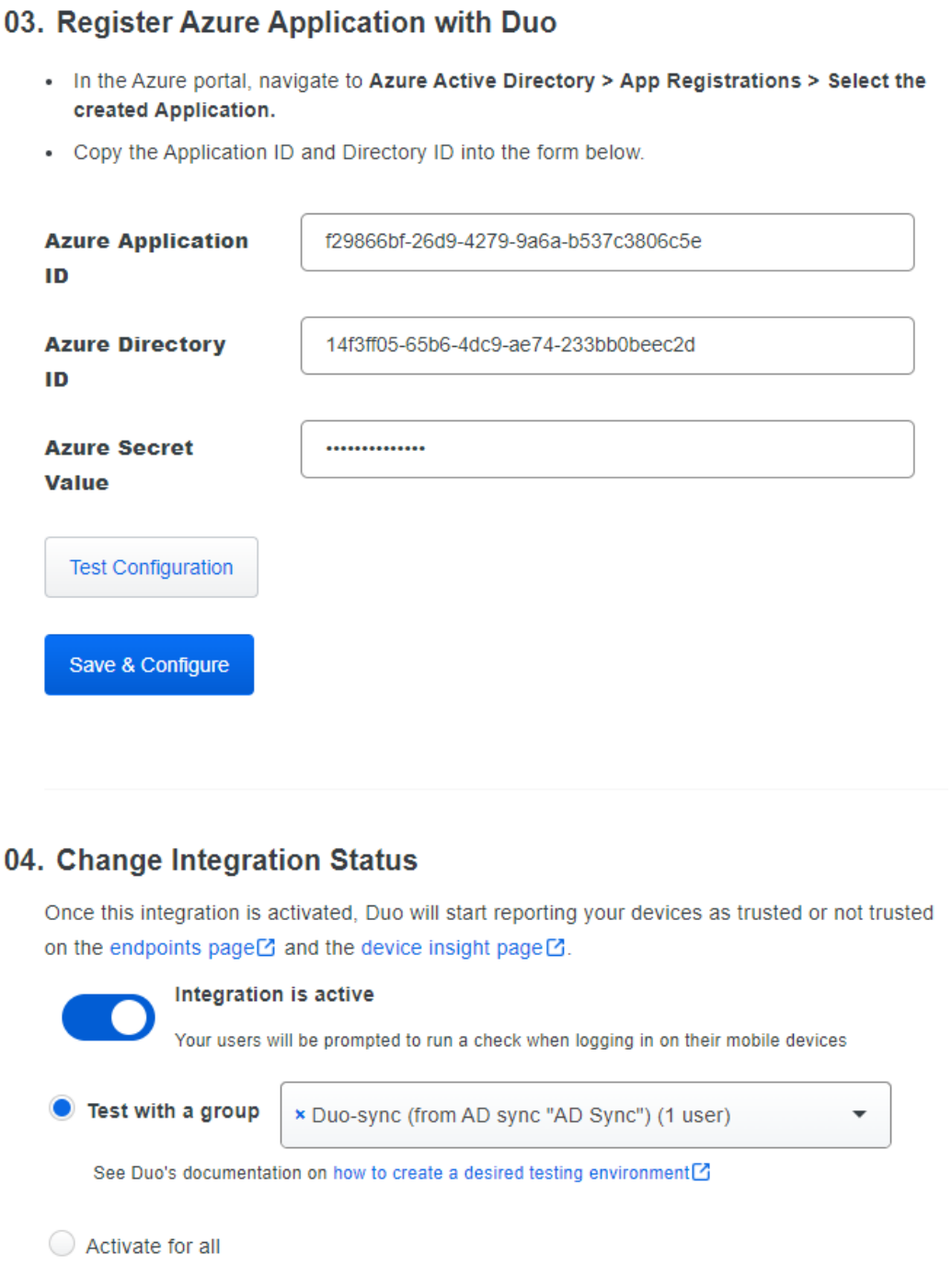
Kuvio 25. Duo Desktop -sovelluksen API luvat Microsoft Azuressa

Luotiin seuraavaksi sovelluksen salaisuus Microsoft Azuressa ja siirryttiin Hallinnoi-osiossa Sovellusten rekisteröinnit -kohtaan sekä valittiin aiemmin luotu Duo-sovelluksen rekisteröinti. Napsautettiin "Varmenne ja salaisuudet" ja lisättiin "Asiakkaan salaisuudet" -kohtaan uusi asiakassalaisuus, jossa on kuvaus ja vanhenemisaika 2 vuotta. Tämä luotu asiakassalaisuus esitetään kuviossa 26. Kopioitiin paljastettu salainen arvo tallennuksen jälkeen, sillä tämä oli ainoa mahdollisuus nähdä se. Tämä salainen arvo on ratkaisevan tärkeä Intunen hallinnan integroinnin määritykselle Duon hallintapaneelissa hallinnan integroinnin määrittämisessä eri käyttöjärjestelmäalustoilla, joten muistettiin säilyttää tämä salaisuus turvallisesti tulevaa käyttöä varten.



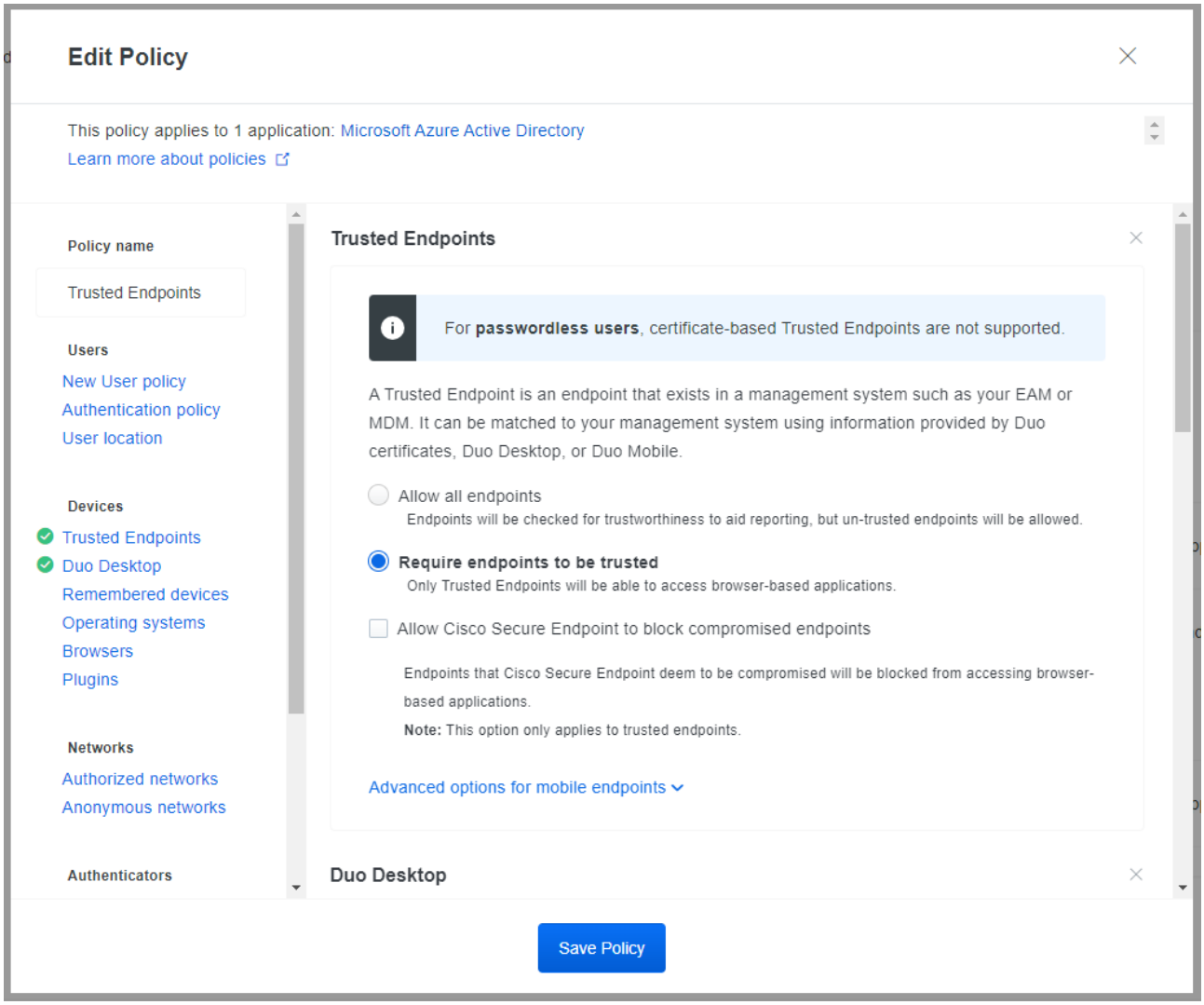
Kuvio 26. Duo Desktop -sovelluksen sertifikaatit & salaisuudet Microsoft Azuressa

Rekisteröitiin Azure-sovellus Duon hallintapaneelissa loppuun kopioimalla Azure-sovellusasiakkaan salainen arvo, joka on luotu Azure-määritysvaiheiden aikana, ja liitettiin se Azure Secret -arvoksi Duon hallintapaneeliin, joka kuvataan kuviossa 27. Siirryttiin sitten Azure-sovelluksen rekisteröinnin yleiskatsaukseen ja kopioitiin sovelluksen tunnus ja vuokralaisen tunnus. Nämä arvot liitettiin Duon hallintapaneeliin Azure Application ID- ja Azure Directory ID -tunnuksiin. Testattiin lopuksi kokoonpanoa varmistaakseen Azure API -käyttö ja valikoitiin Tallenna & Määritä, kun testaus onnistui. Vaihdettiin integroinnin tila aktiiviseksi onnistuneen konfiguraation testauksen jälkeen ja määritettiin integroinnin testaus TESTISRV1 AD:lla olevan Duo-sync -ryhmän kanssa.



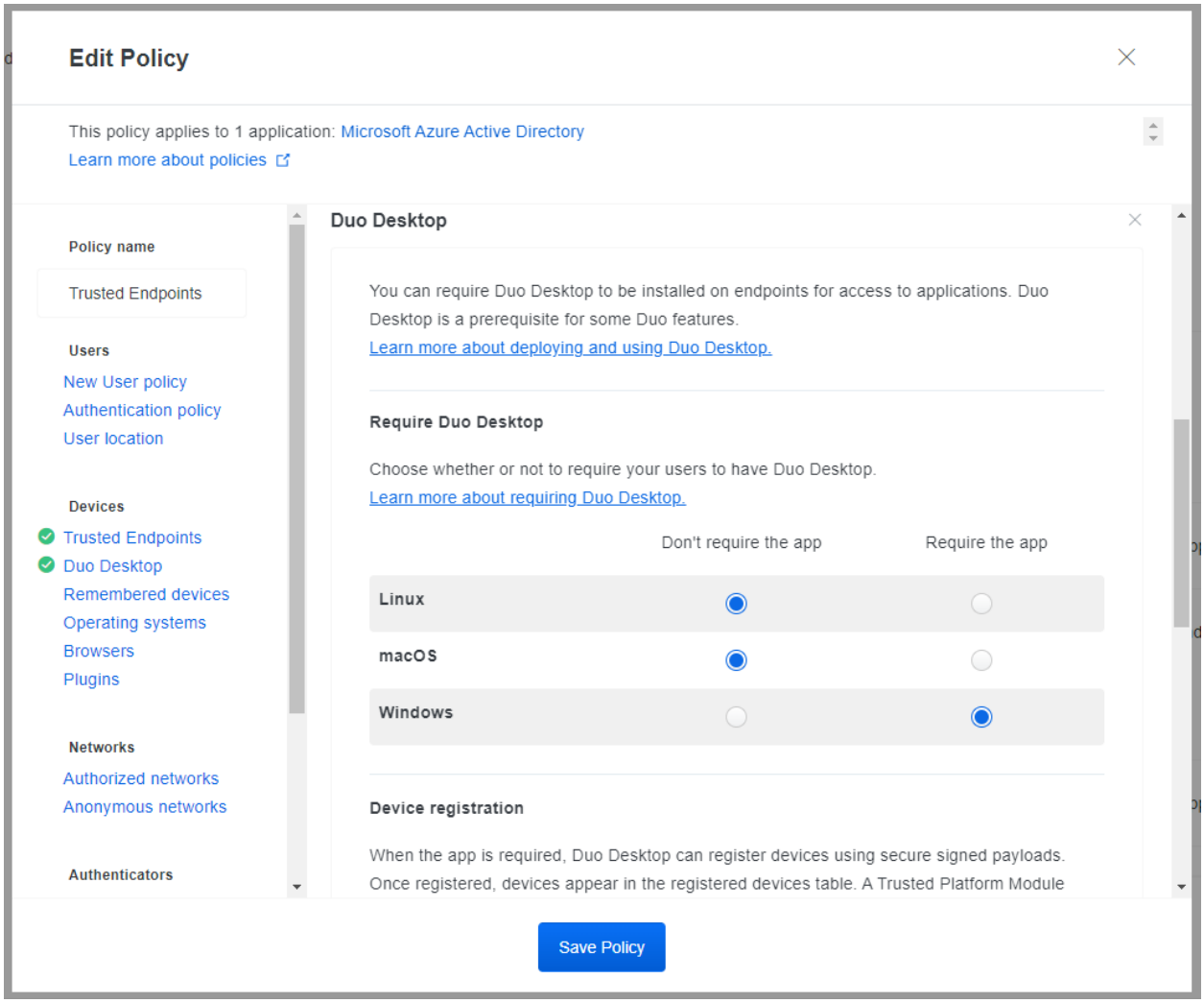
Kuvio 27. Intune with Duo Desktop -integraation rekisteröinti ja integrointi tilan muuttaminen

Muokattiin Duon hallintapaneelissa Microsoft Azure Active Directory -sovelluksen käytäntöihin Trusted Endpoints käyttöön ja nähtiin samalla, että se piti sisällään samalla äskettäin siihen luodun Duo Desktop integraation. Kuviossa 28 nähdään, että muokattiin käytäntöjä siten, että vaadittiin kaikkien päätepisteiden olevan luotettuja.



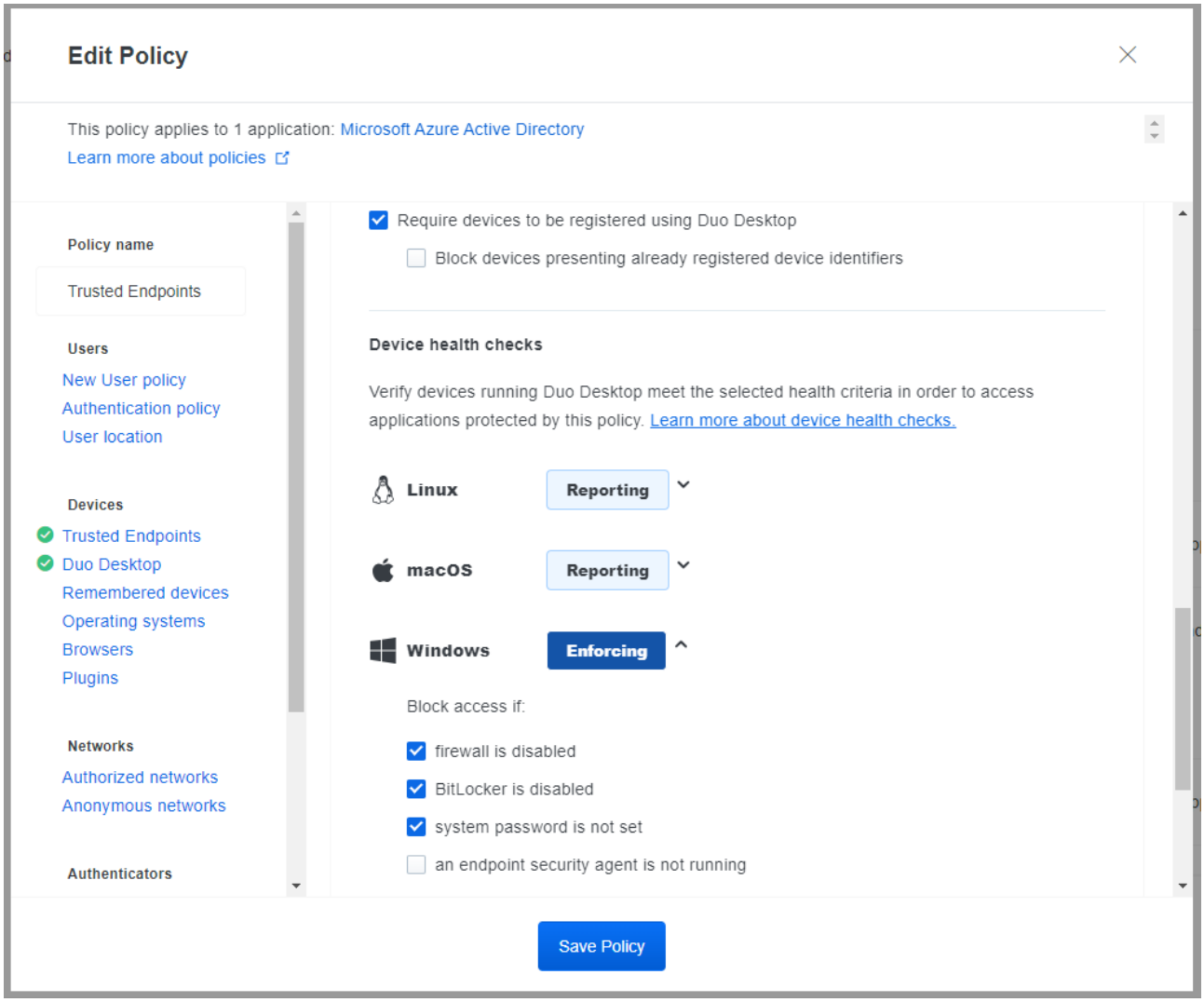
Kuvio 28. Duo Trusted Endpoints -käytännön vaatiminen

Kuviossa 29 nähtävässä kohdassa vaadittiin Duo Desktop käyttöön tässä tilanteessa vain Windows-järjestelmillä oleville päätepisteille, koska ympäristössä ei ollut muiden käyttöjärjestelmien päätepisteitä.



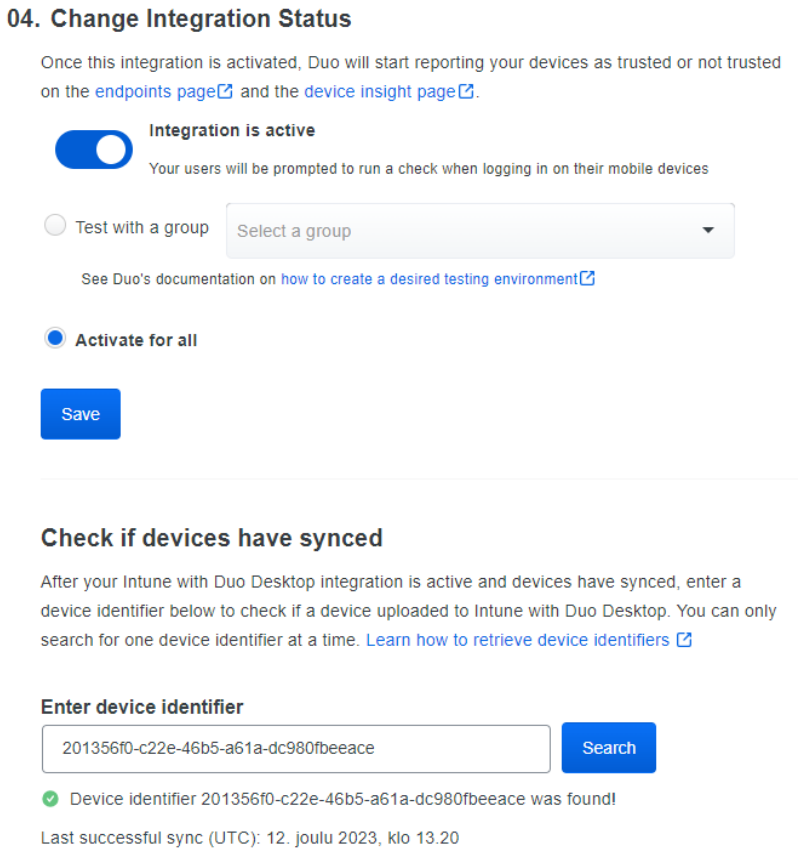
Kuvio 29. Duo Desktop -sovelluksen vaatiminen Windows-järjestelmissä

Kuviossa 30 on kohta, jossa asetettiin Duo Desktopin Device health tarkastukset pakotetusti Windows-järjestelmillä oleville päätepisteille ja sillä ehdoin, että pääsy estetään, jos palomuuri sekä BitLocker on poissa käytöstä ja järjestelmään ei ole asetettu salasanaa. Ei pakotettu viimeistä ehtoa liittyen päätepisteen suojaus agentin käynnissä olemiseen, koska päätepisteillä on käytössä toinen virustorjunta Windows Defenderin sijasta, mitä ei tueta ainakaan vielä tässä Cisco Duon kehitysvaiheessa. Tallennettiin lopuksi muokattu käytäntö sovellukseen käytettäväksi. Vaadittiin lisäksi, että päätepisteet täytyy olla rekisteröity Duo Desktopilla, jotta kirjautuminen onnistuu. Sovellettiin tätä muokattua käytäntöä jälleen vain Duo-sync -ryhmälle.



Kuvio 30. Duo Desktop -käytännön Device health checks pakotus Windowsissa

Määritettiin lopuksi integrointi aktiiviseksi kaikille, koska todettiin sen olleen toiminut Duo-sync -ryhmän kohdalla. Tarkistettiin vielä Intune with Duo Desktop konfiguraation jälkeen, oliko ympäristön testilaite ladattu Intune with Duo Desktopin avulla, joka juuri konfiguroitiin ympäristön Microsoft Azureen. Haettiin päätepisteen tunniste, joka löytyi Microsoft Azuren kautta Intune-hallinnasta päätepisteen tiedoista. Syötettiin tunniste konfiguraation tarkistuskohtaan ja kuviossa 31 on kuvattu, että haku löysi vastaavuuden kyseisellä laitetunnisteella. Voitiin todeta, että integroinnin konfigurointi on onnistunut ja yhteys oli syntynyt Duon ja Intunen välille.

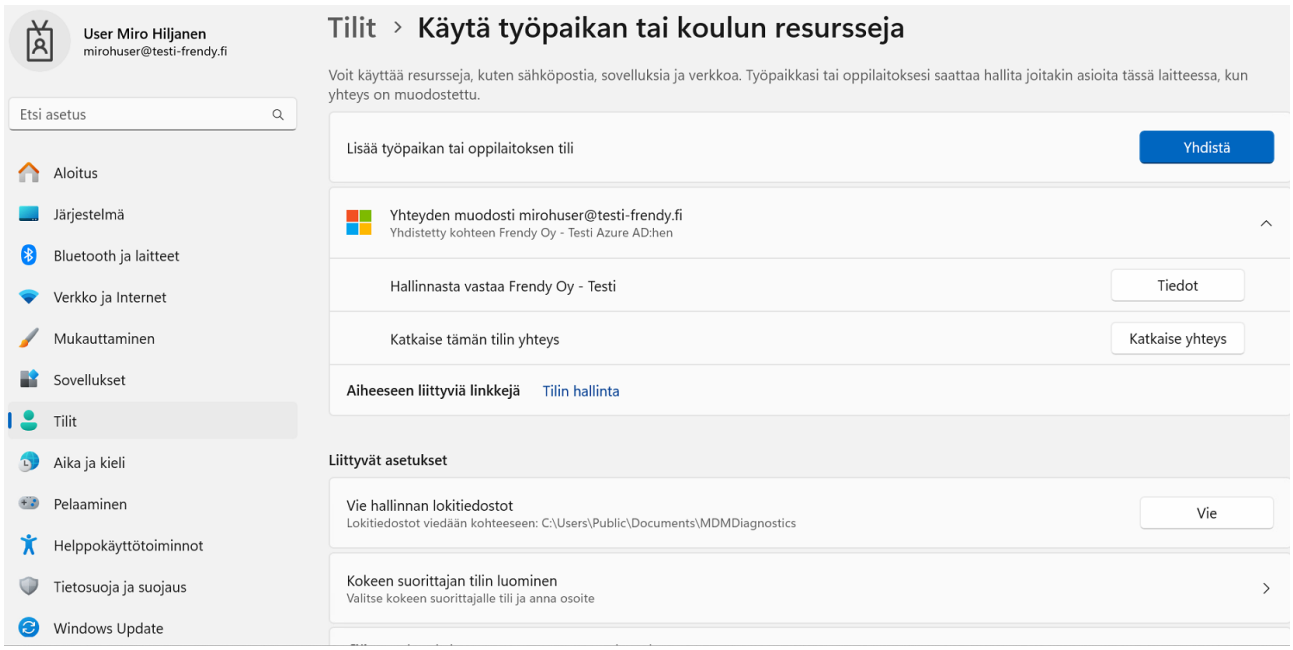


Kuvio 31. Intune with Duo Desktop -integroinnin tilan muuttaminen ja päätepisteen synkronoinnin tarkistus

8.8 Päätepisteen yhdistäminen Microsoft Entra -vuokralaiseen

Laitehallintaa Microsoft Entra ID:n avulla vaaditaan, kun Windows 11 -laite yhdistetään Microsoft Entra -vuokralaiseen. Tämä toimenpide suoritetaan yleensä Out-of-Box Experiencen aikana, joka on päätepisteen ensimmäinen asennus. Käyttäjät voivat valita sopivan organisaation tilin tämän asennuksen aikana yhdistääkseen tämän päätepisteen Microsoft Entra -vuokraajaan. Tämän linkin kautta päätepistettä voidaan hallita keskitetysti Microsoft Entra ID:n kautta, mikä helpottaa nopeaa pääsyä organisaatioresursseihin ja turvamääräysten yhtenäistä täytäntöönpanoa. Tämä menettely on erityisen tärkeä yritysasetuksissa, joissa käyttäjien ja laitehallinta on keskitetty turvallisuuden ja tehokkuuden vuoksi. (Microsoft Entra join a new Windows device during the out of box experience 2023.)

Päätettiin liittää päätepiste vasta Windows 11 asennuksen jälkeen eikä edellä kuvatulla OOBE-tavalla. Avattiin päätepisteeltä Windows tilit -asetukset ja valikoitiin työpaikan tai koulun resurssien käyttö. Yhdistettiin uusi työpaikan tai oppilaitoksen tili antamalla vuokralaisella olevan käyttäjän sähköpostiosoite ja salasana, jonka jälkeen valittiin ”Liitä tämä laite Azure Active Directoryyn”. Vahvistettiin liitos ja saatiin vahvistus onnistumisesta, jonka jälkeen kuviossa 32 nähdään aktiivinen yhteys päätepisteen Windowsin tilit-asetuksissa vielä vanhalla Azure AD nimellä.



Kuvio 32. Päätepisteen yhdistys Microsoft Entra ID -vuokralaiseen

8.9 Duo Desktop -sovelluksen asennus päätepisteelle

Kuten kappaleessa 5.4.2 kerrotaan, Duo Desktop parantaa organisaatioiden hallintaa sovellusten käyttöoikeuksien osalta. Se tekee tämän arvioimalla päätepisteiden suojausasentoa ja varmistamalla Duo Desktopin läsnäolon. Duo Desktop koostuu kolmesta osasta: natiivi asiakassovellus, lisätiedot päätepisteistä sen hallintapaneelin kautta, ja käyttöoikeuskäytännöt päätepisteen kunnon mukaan. Käyttäjien on asennettava Duo Desktop, jonka jälkeen ohjelma estää epäterveiden päätepisteiden kirjautumisen ja opastaa käyttäjiä parantamaan päätepisteidensä tietoturvan tasoa. Turvallisuusriskit liittyvät tiedon yksilöimättömyyteen, mutta yksilöllisten todentamistunnusten ja päätepisterekisteröinnin käyttö voi vähentää näitä riskejä.

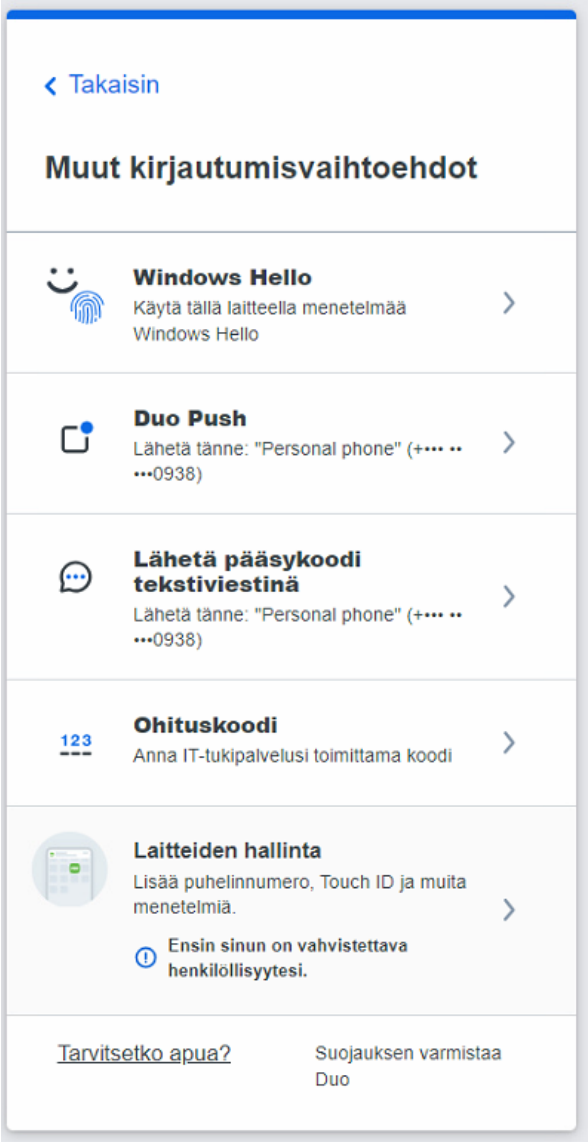
Kun Duo Trusted Endpoints -käytäntö ja Intune with Duo Desktop on konfiguroitu, seuraava vaihe Microsoft Azure Active Directory -sovelluksen asettamisessa Duon hallintapaneelissa on Duo Desktopin asentaminen testausta varten. Tämä asennus on osa alkuperäistä Duon määritystä. Kun laite, jota käytetään kirjautumiseen, kuuluu Microsoft Entra -vuokraajaan ja on yhdistetty Duon hallintapaneelissa luotuun sovellukseen niin Duo Desktop asennetaan automaattisesti ennen Office 365 -kirjautumista. Aloitettiin lataamalla sovellus päätepisteelle ja asennettiin se. Tämän jälkeen se pysyy aina taustalla valmiina avautumaan kirjautumista varten, ja se tarkkailee jatkuvasti aiemmin määritettyjen ehtojen täyttymistä. Myöhemmin tarkistetaan myös Duo Desktopin toiminta perusteellisesti.

9 Toteutuksen testaus

Monivaiheisen todentamisen toteutuksen testaus on keskeinen osa tämän opinnäytetyön käytännön soveltamista. Testausvaihe tarjoaa syvällistä ymmärrystä siitä, kuinka Duon monivaiheisen todentamisen järjestelmä toimii käytännössä ja miten se integroituu yrityksen olemassa olevaan tietoturvaympäristöön. Tässä luvussa tarkastellaan yksityiskohtaisesti testausprosessin eri vaiheita, mukaan lukien Cisco Duon konfigurointi, käyttöönotto ja käytännön testit. Testauksen tulokset tarjoavat arvokasta tietoa siitä, kuinka järjestelmä käyttäytyy todellisissa käyttöolosuhteissa ja miten se vastaa asetettuihin tietoturva- ja käytettävyysvaatimuksiin.

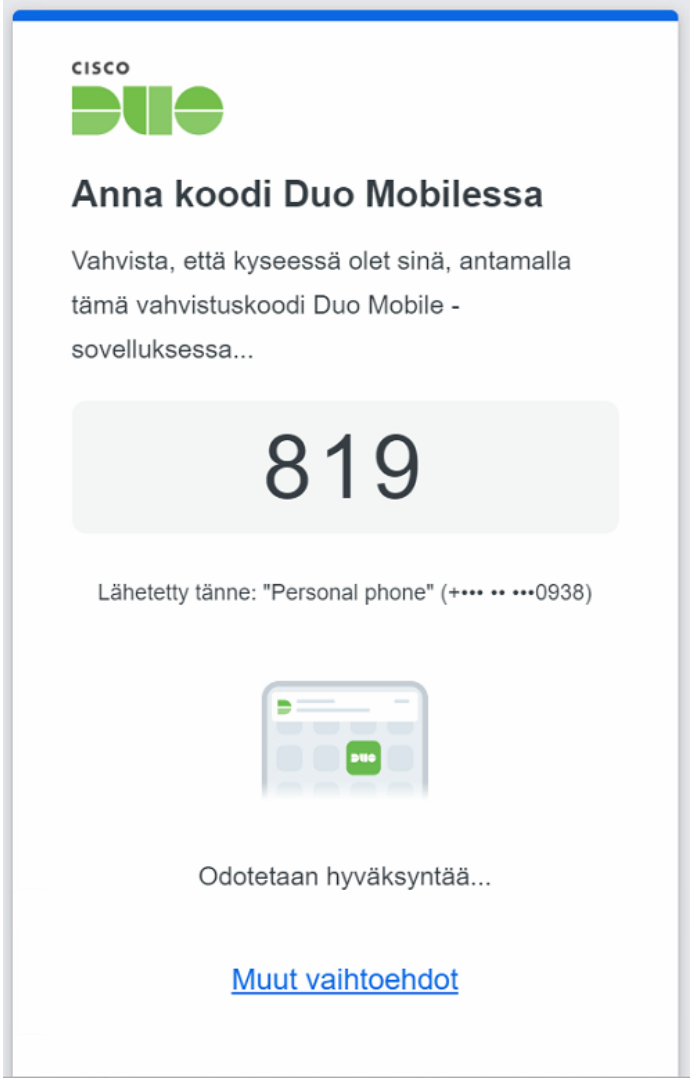
9.1 Kirjautuminen Duolla

Aiemmassa 8.6 luvussa tehtiin ja kuvattiin jo Duo Securityn sekä Duo Mobilen käyttöönotto, joten voitiin sen pohjalta seuraavaksi testata kirjautumista käytännössä. Toteutettiin se yksinkertaisesti niin, että kirjauduttiin testitunnuksella portal.office.com -sivuston kautta Office 365:een, joka oli määritetty kokonaisuudessaan Microsoft Entran ehdollisen pääsyn kohteeksi. Kuviossa 33 huomataan, että tunnusten syöttämisen jälkeen meille avautui kirjautumisvaihtoehdot, joka pyysi oletuksena käyttämään Windows Helloa, koska se oli asetettu 8.6 luvussa kirjautumisvaihtoehdoista oletukseksi.



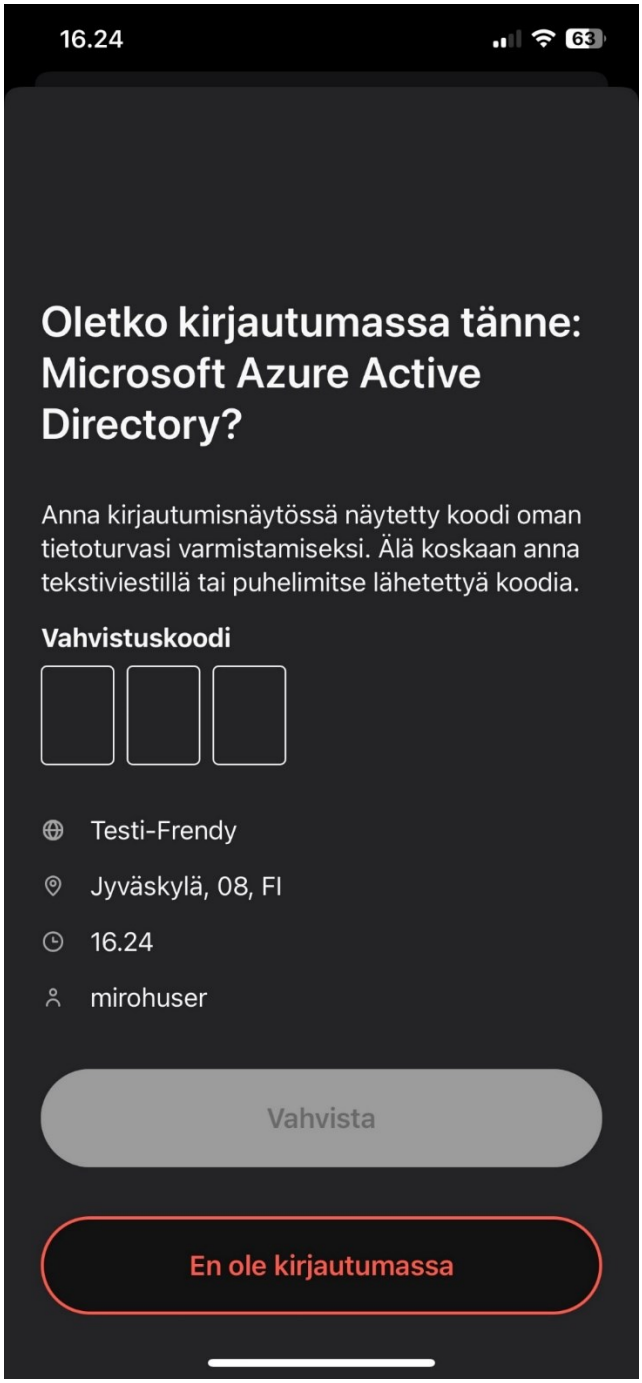
Kuvio 33. Duo MFA:n kirjautumisvaihtoehdot

Käytettiin kuitenkin Duo Push -kirjautumisvaihtoehtoa kirjautumiseen ja kuviossa 34 on pyyntö vahvistaa kirjautuminen kehotteessa näkyvällä vahvistuskoodilla puhelimen Duo Mobile -sovelluksessa, joka oli jo aiemmin asennettu puhelimeen.



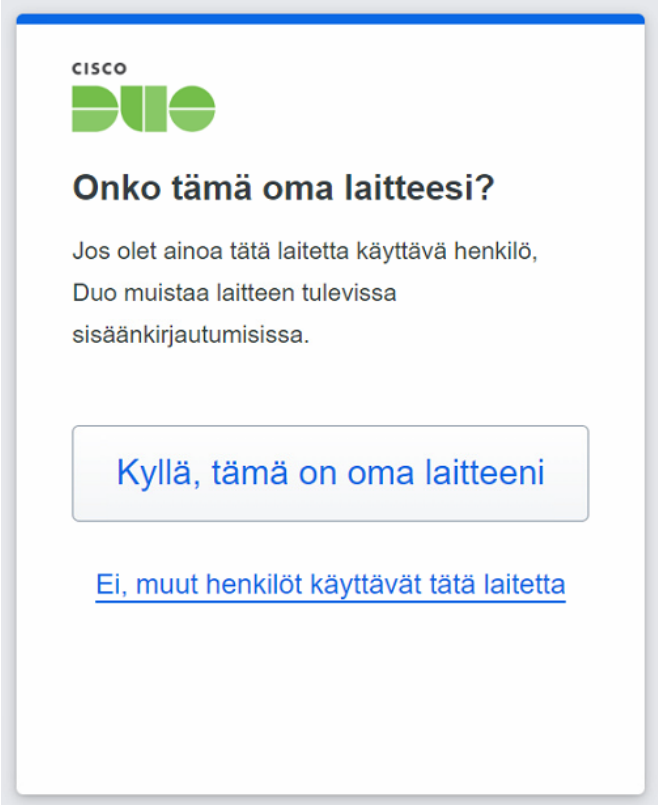
Kuvio 34. Duo Mobile -sovelluksen vahvistuskoodi

Avattiin puhelimesta Duo Mobile -sovellus ja sinne tulleesta kirjautumisen ilmoituksesta voitiin todeta verkkosivuston, sijainnin, kellonajan ja käyttäjätunnuksen perusteella, että kyseessä oli oikea ilmoitus kirjautumisesta, joten syötettiin kirjautumispäätepisteellä nähty vahvistuskoodi Duo Mobilen vahvistusikkunaan ja vahvistettiin kirjautuminen. Halutessaan pystyttiin kieltäytymään kirjautumisesta, mikäli kuviossa 35 näkyvät ilmoituksen tiedot vaikuttaisivat oudoilta, jolloin mahdollinen hyökkääjä ei pääsisi käyttäjän tunnuksella kirjautumaan.



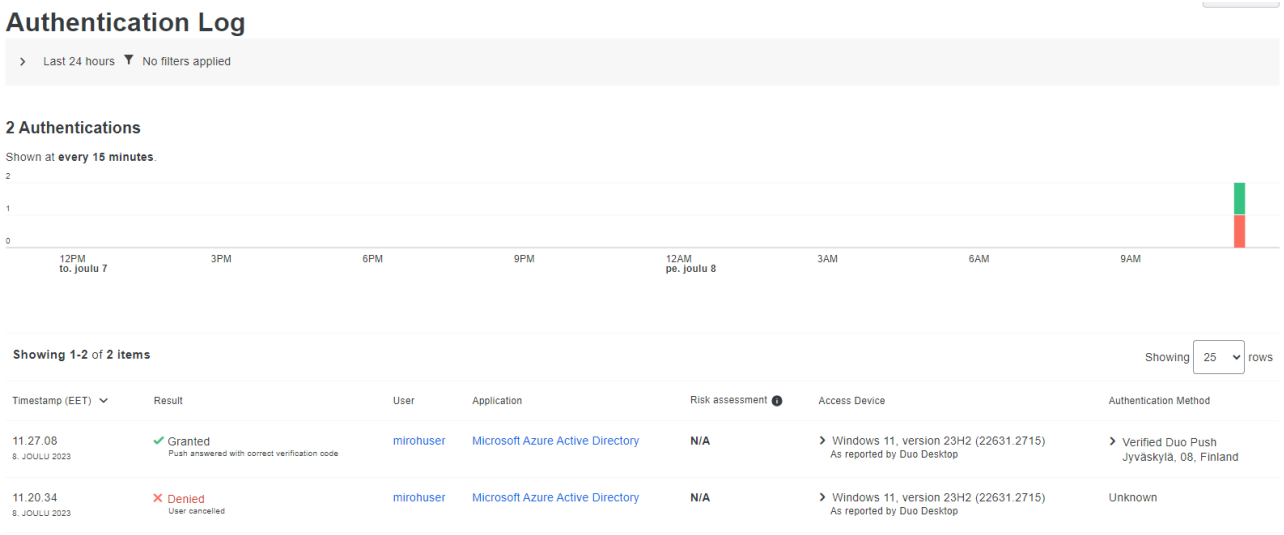
Kuvio 35. Duo Mobile -sovelluksen push-ilmoitus iOS-laitteessa

Kuviossa 36 nähdään päätepisteellä oleva ilmoitus, joka saatiin Duo Mobilessa olevan kirjautumisen vahvistamisen jälkeen ja siinä kysytään, oliko kyseessä käyttäjän oma laite vai muillakin käytössä oleva laite. Riippuen vastauksesta Duo muistaa päätepisteen jatkossa käyttäjän kirjautumissa suoraan tai sitten se kysyy tätä aina uudelleen, jonka jälkeen Duo kirjaa käyttäjän sisään.



Kuvio 36. Päätepisteen rekisteröinti Duo MFA:n kirjautumisessa

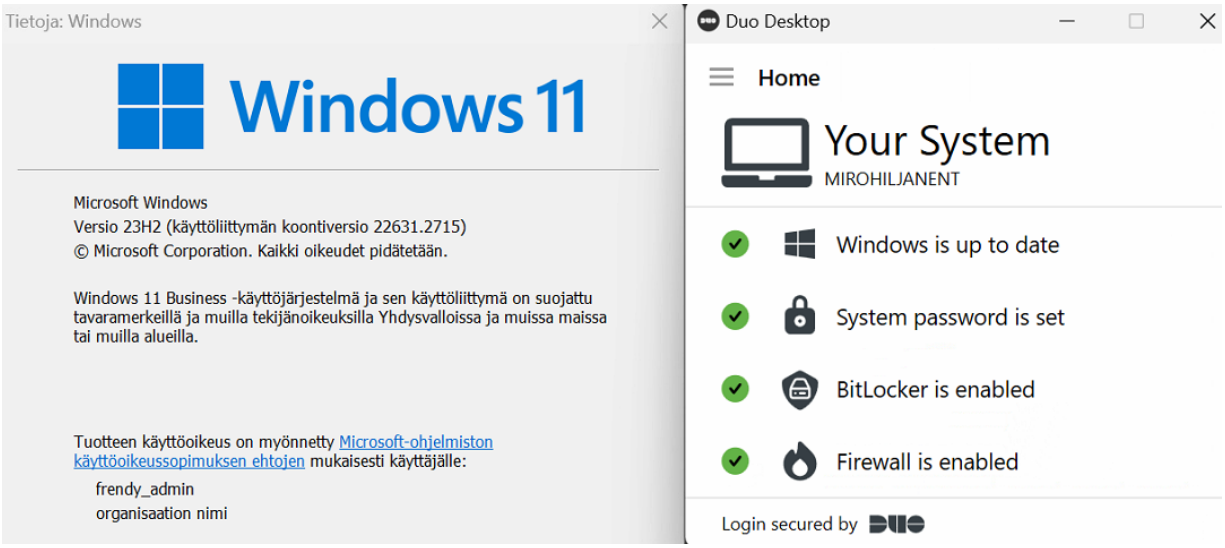
Pystyttiin toteamaan kirjautumisen onnistuminen tai epäonnistuminen kuviossa 37 nähtävän Cisco Duon hallintapaneelin todennuslokin kautta. Nähtiin todennuslokista ensimmäisessä kirjautumisessa, että se on estetty, koska testattiin perua kirjautuminen. Toisella kerralla testattiin kirjautua loppuun asti ja nähtiin, että se on tullut myös todennuslokiin näkyviin onnistuneena kirjautumisena, jossa on käytetty todentamismenetelmänä nimenomaan varmistettua Duo Push -kirjautumisvaihtoehtoa, koska valikoitiin päätepisteen olevan oma päätepiste.



Kuvio 37. Authentication Log -näkymä Duossa

9.2 Kirjautuminen Duo Desktopilla

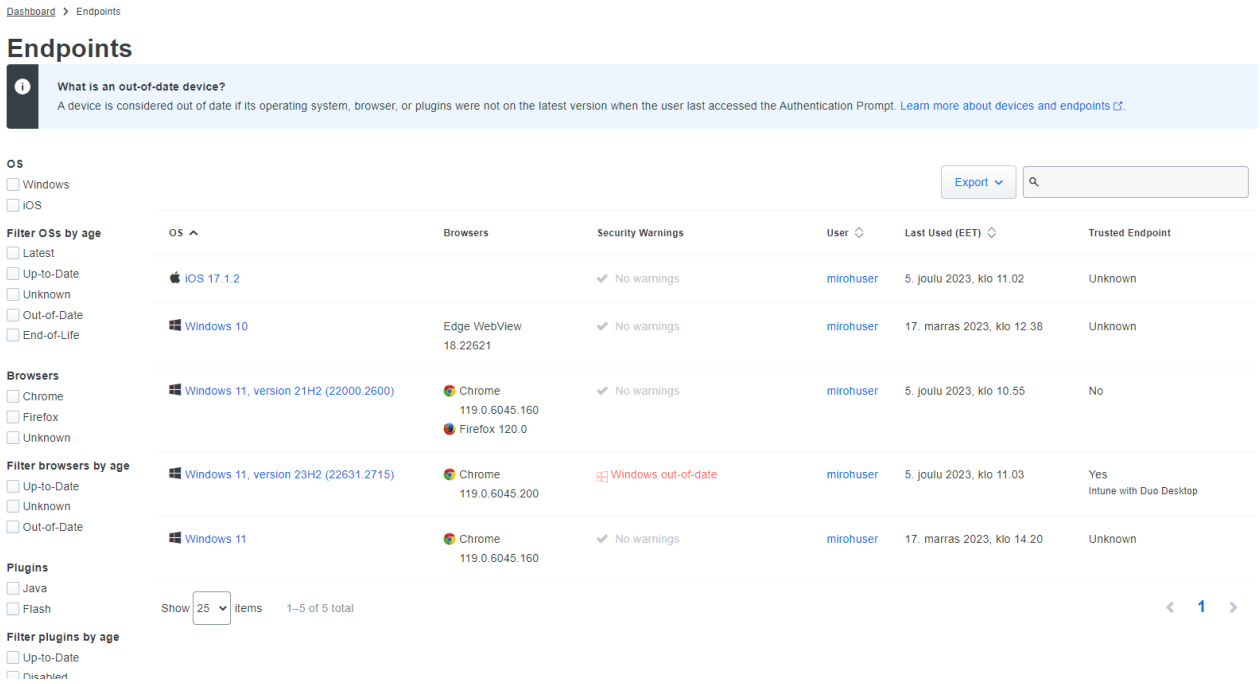
Seuraavaksi testattiin kirjautumista käyttäen lisänä Duon Trusted Endpoints -käytäntöä, joka oli jo aiemmin määritetty ympäristöön ja näkyikin aiemmassa MFA:n kirjautumisessa. Kirjauduttiin jälleen portal.office.com -sivuston kautta Office 365:een ja saatiin kehote ladata tai avata Duo Desktop. Avattiin Duo Desktop, koska se oli valmiiksi asennettu päätepisteelle ja se lähti käynnistymään sekä tarkistamaan päätepisteen suojausta. Saatiin Duo Desktopilta ilmoitus, että toiminto tarvitaan, koska päätepisteen Windows ei ollut ajan tasalla. Päivitettiin päätepisteen Windows ajan tasalle ohjeiden mukaan ja varmistettiin sitten päätepisteen Duo Desktopin kertovan, että Windows oli ajan tasalla, salasana oli asetettu, BitLocker sekä palomuuri oli käytössä. Kuviossa 38 nähdään vihreiden symbolien kertovan kaiken olevan päätepisteellä kunnossa. Päästiin onnistuneen Duo Desktop tarkastusten jälkeen valikoimaan normaalisti kirjautumisvaihtoehtoista menetelmä, jolla halutaan kirjautua sisään ja sen jälkeen kirjautuminen noudatti samoja vaiheita kuin normaali Cisco Duo MFA:n kirjautuminen.



Kuvio 38. Päätepisteen Windows-version tarkistus ja Duo Desktopin tarkistukset

9.3 Päätepisteen tarkastelu ja hallinta Duossa

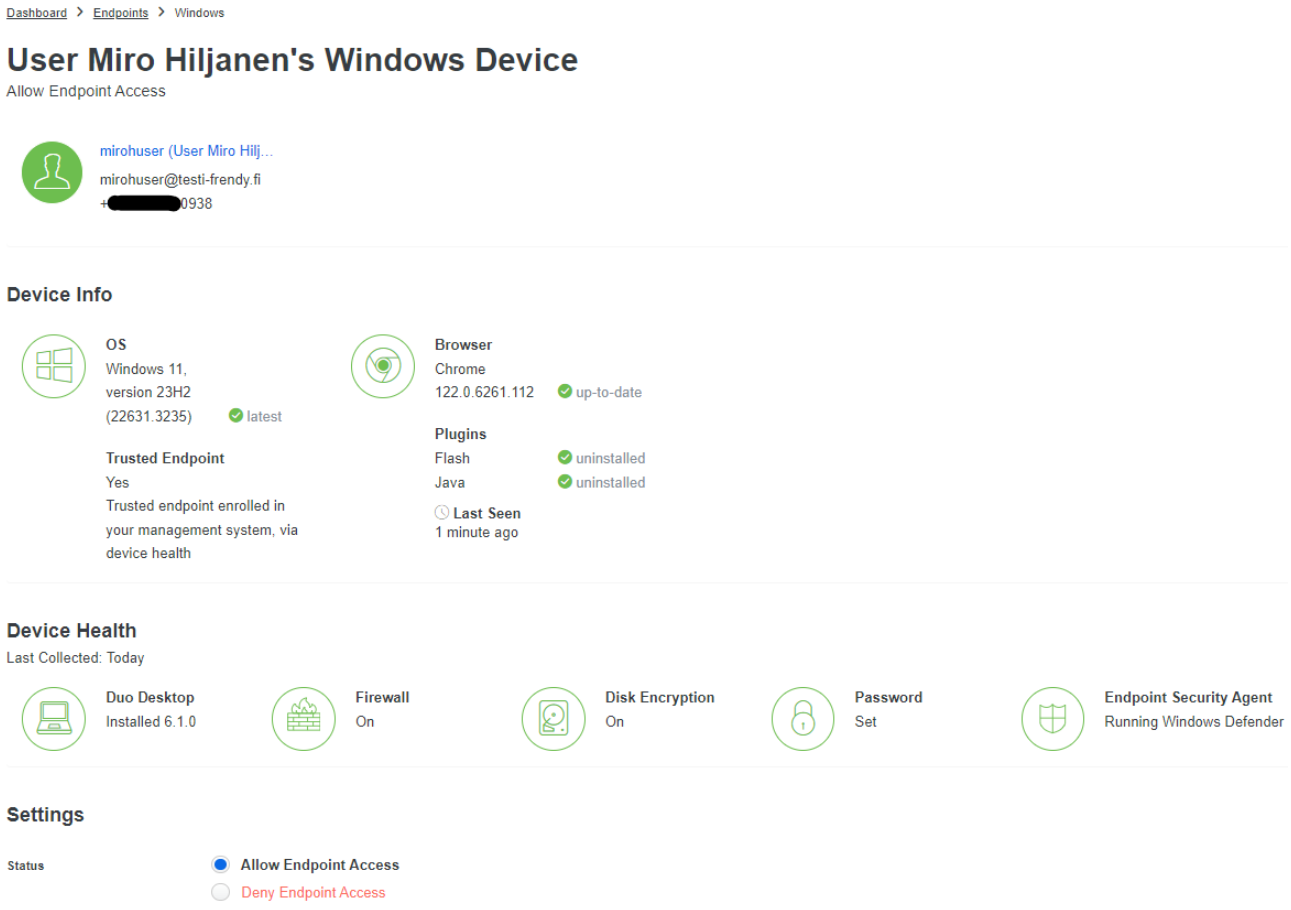
Cisco Duon hallintapaneeli mahdollistaa päätepisteiden tarkastelun ja hallinnan monella eri tavalla. Kuviossa 39 nähdään hallintapaneelissa olevat kaikki järjestelmään rekisteröidyt päätepisteet. Tämä sisältää tiedot päätepisteen tyypistä, käyttöjärjestelmästä, ja viimeisimmästä käyttöajankohdasta. Nähdään myös, mitkä niistä ovat aktiivisia ja mitkä eivät. Voidaan tarkistaa kunkin päätepisteen turvallisuustila, kuten onko siinä käytössä uusimmat turvapäivitykset ja käyttöjärjestelmän versiot. Duon hallintapaneelin kautta voidaan määritellä, mitkä päätepisteet saavat pääsyn tietyille palveluille tai sovelluksille. Voidaan myös asettaa käyttöoikeuksiin liittyviä käytäntöjä, jotka määrittelevät, millaisilla päätepisteillä on oikeus päästä tiettyihin tietoihin. Jos päätepiste on kadonnut tai ei enää ole käytössä, voidaan poistaa se Duon hallintapaneelin kautta järjestelmästä, joka estää tietoturvariskit. Duo tarjoaa yksityiskohtaisia raportteja ja lokitietoja päätepisteiden käytöstä ja näistä raporteista nähdään, miten ja milloin eri päätepisteitä on käytetty todentamiseen. Voidaan asettaa hälytyksiä epätavallisesta toiminnasta, kuten epäonnistuneista kirjautumisyrityksistä tai uusien päätepisteiden rekisteröinneistä.



Kuvio 39. Endpoints-näkymä Duossa

Esimerkiksi Duon Trusted Endpoints -käytäntöä käyttäviä päätepisteitä ja niiden kirjautumisia pystyttiin hyvin tarkastelemaan ja hallinnoimaan Duon hallintapaneelin Endpoints-näkymän kautta. Huomattiin, että äskettäinen kirjautuminen Duo Desktopin avulla oli rekisteröitynyt sinne yhden päätepisteen kohdalle ja nähtiin sen sisältävän varoituksia koskien muun muassa päätepisteen vanhentunutta Windowsin ja Chromen versiota. Myöhemmin tarkasteltuna voitiin kuitenkin todeta, että varoitus oli hävinnyt kyseisen päätepisteen kohdalta, koska päätepisteeseen suoritettiin ohjeiden mukaiset Windowsin ja Chromen päivitykset. Rekisteröidyiksi päätepisteeksi valitulta päätepisteeltä pystyttiin halutessaan myös poistamaan rekisteröinti, jolloin käyttäjä joutui kirjautumisen yhteydessä valikoimaan rekisteröinnin uudelleen eikä kirjautuminen tapahtunut suoraan niin helposti.

Duon käytännöllä ei estetty kokonaan kirjautumisia vaan, jos Duo Desktopin tarkistus ei onnistunut se pystyttiin ohittamaan ja kirjautumaan sisään. Tästä saatiin kuitenkin ilmoitus Duon hallintapaneeliin päätepiteen kohdalle. Järjestelmänvalvojana kykeni tarkastelemaan kuviossa 40 näkyvää esimerkkipäätepistettä tarkemmin nähden käytettävän käyttöjärjestelmän, selaimen ja päätepisteen kuntotarkastuksen pitäen sisällään Duo Desktopin asennuksen, palomuurin, levyn salauksen, salasanan asetuksen ja päätepisteen suojausagentin tarkistukset.



Kuvio 40. Esimerkkipäätepisteen tarkemmat tiedot Duossa

10 Pohdinta

10.1 Yrityksen tarpeeseen lähestyminen

Opinnäytetyössä lähestyttiin toimeksiantajan tarvetta parantaa tietoturvaa monivaiheisen todentamisen käyttöönotolla. Toimeksiantajayritys Frendy toimi laajasti Suomessa tarjoten IT-palveluita. Yrityksen tavoitteena oli tutkia nimenomaan Cisco Duon monivaiheisen todentamisen soveltuvuutta Frendyn asiakaskunnalle, erityisesti pienille ja keskisuurille yrityksille, joilla ei ole mahdollista käyttää Microsoft Entra ID:tä. Työssä korostettiin Cisco Duon integroitumista yrityksen olemassa oleviin Cisco-palveluihin ja sen merkitystä Frendyn tietoturvan parantamisessa. Käyttöönottoprosessi sisälsi järjestelmän testaamisen yrityksen testiympäristössä keskittyen kirjautumisprosessin toimivuuteen ja käyttöönoton perusteisiin tukien näin Frendyn pyrkimyksiä kohti tietoturvallista toimintaa.

Projekti alkoi kartoituksella, jossa tunnistettiin yrityksen kohtaamat mahdolliset tietoturvaongelmat ja määriteltiin ratkaisuksi Cisco Duon käyttöönotto testausympäristöön. Yhteistyössä Frendyn kanssa suunniteltiin tekninen toteutus ja järjestelmän testaus. Tavoitteena oli luoda vankka tietoturvaympäristö, joka suojaa yritysten arkaluonteisia tietoja ja parantaa käyttäjäkokemusta modernilla todentamismenetelmällä. Työssä korostettiin monivaiheisen todentamisen merkitystä tietoturvan kannalta ja sen integroinnin vaikutuksia yrityksen tietoturvapolitiikkaan.

10.2 Saadut toimintatulokset ja johtopäätökset

Työn perusteella Cisco Duon monivaiheinen todentaminen osoittautui tehokkaaksi ja onnistuneeksi menetelmäksi käyttäjien henkilöllisyyden varmistamisessa. Se yhdistää useita todentamismenetelmiä, kuten biometriset varmennustekniikat, suojaustunnukset ja salasanat luoden näin monitasoisen suojan. Uudet teknologiat, kuten tekoäly ja koneoppiminen, avaavat uusia mahdollisuuksia parantaa tämän järjestelmän turvallisuutta ja käyttäjäystävällisyyttä. Kuitenkin samalla monivaiheinen todentaminen tuo mukanaan käyttäjäkokemuksen haasteita, kuten prosessin monimutkaisuuden tai käyttäjien vastustuksen, jotka ovat tärkeä ottaa huomioon.

Tulokset osoittavat, että on välttämätöntä löytää tasapaino tietoturvan parantamisen ja käyttäjäystävällisyyden säilyttämisen välillä. Käyttöliittymäsuunnittelu ja käyttäjäkoulutus ovat keskeisiä tekijöitä tämän tasapainon saavuttamisessa. Lisäksi teknologian jatkuva kehitys vaatii monivaiheisen todentamisen jatkuvaa päivitystä ja mukauttamista uusiin uhkiin ja mahdollisuuksiin. Tämä korostaa tarvetta noudattaa tietoturvastandardeja ja lainsäädäntöä monivaiheisen todentamisen kehittämisessä ja toteutuksessa.

Tulevaisuudessa monivaiheinen todentaminen tarjoaa laajoja mahdollisuuksia parantaa tietoturvaa eri aloilla ottaen huomioon teknologian kehityksen ja muuttuvat tietoturvauhat. Monivaiheisen todentamisen soveltaminen voi olla avainasemassa tietoturvallisuuden parantamisessa monenlaisissa organisaatioissa. Sen soveltamisalueiden laajentaminen ja jatkuva kehitys ovat välttämättömiä tietoturvariskien hallinnassa ja käyttäjien turvallisen digitaalisen kokemuksen takaamisessa.

10.3 Opinnäytetyön tavoitteet

Kuten aiemmin mainittiin, Frendyn intresseissä oli tutkia Cisco Duo monivaiheisen todentamisen soveltuvuutta asiakkailleen keskittyen erityisesti pieniin ja keskisuuriin yrityksiin, jotka eivät käytä Microsoft Entra ID:tä tai joilla ei ole käytössä tähän tarvittavia lisenssejä. Tämä opinnäytetyö pyrki syventämään ymmärrystä Cisco Duon soveltuvuudesta Frendyn asiakkaille ja integroitumisesta yrityksen olemassa oleviin Ciscon palveluihin, joita vahvistaa pitkäaikainen kumppanuus Ciscon kanssa. Tavoitteena on myös kehittää ja dokumentoida Cisco Duon monivaiheisen todentamisen käyttöönotto Frendyn testiympäristössä ennen sen siirtoa tuotantoon tarkkaillen erityisesti kirjautumisprosessin eri vaiheita ja perusteita sen käyttöönotolle. Työllä on keskeinen merkitys Frendyn tietoturvallisten tavoitteiden ja hallintastandardien saavuttamisessa.

Tietoturvallisuuden ja tietomurtojen merkitys nykypäivän yhteiskunnassa on merkittävä, ja ne vaikuttavat laajasti yksilöihin, yrityksiin sekä yhteiskuntaan kokonaisuudessaan. Tässä työssä keskitytään erityisesti siihen, kuinka Cisco Duon monivaiheinen todentaminen, joka keskittyy käyttäjän tunnistamiseen ja pääsynhallintaan voi auttaa Frendyä suojaamaan tietojaan ja verkkojaan nykyajan teknologian tuomilta uusilta uhilta ja haasteilta. Cisco Duon monipuoliset työkalut auttavat varmistamaan, että vain oikeilla käyttäjillä on pääsy tietoverkkoihin ja -järjestelmiin, mikä erottaa sen kilpailijoistaan. Frendyn tietoturvaosaston asiantuntemus ja alustan toiminnallisuudet olivat keskeisiä tekijöitä päätöksenteossa ottaa käyttöön Cisco Duon monivaiheinen todentaminen, joka on suunniteltu toimimaan yhdessä Microsoft Entra ID:n kanssa. Tämä valinta tuki projektin alkuperäistä tavoitetta tarjota pienille ja keskisuurille yrityksille joustava ja tulevaisuuteen katsova turvallisuusratkaisu, joka ei edellytä Microsoft Entra ID:n välitöntä käyttöä mutta mahdollistaa saumattoman integraation tarvittaessa. Tämän strategian myötä pyritään varmistamaan, että tarjotaan yrityksille paitsi nykyhetken turvallisuustarpeisiin vastaava ratkaisu myös valmiuden tulevaisuuden teknologiaintegraatioille edistäen näin turvallisuuden joustavuutta ja skaalautuvuutta.

Monivaiheinen todentaminen on noussut olennaiseksi osaksi nykyaikaista tietoturvaa, ja sen rooli tässä opinnäytetyössä on merkittävä. MFA vaatii käyttäjän todistamaan henkilöllisyytensä useamman kuin yhden tai kahden todentamisvaiheen kautta, mikä tarjoaa merkittävästi korkeamman turvallisuustason. MFA:n käyttöönotto vähentää huomattavasti luvattoman pääsyn riskiä tietojärjestelmiin, jopa silloin, kun yksi todentamistaso murretaan. Tämän projektin tavoitteena oli tutkia, miten Cisco Duon monivaiheisen todentamisen käyttöönotto Frendyn testiympäristössä parantaa

tietoturvaa ja suojaa käyttäjiä sekä tietoja verrattuna jo käytössä olevaan Microsoft Entra MFA:han. Tämä käyttöönotto korosti Cisco Duo MFA:n merkitystä tehokkaana keinona parantaa tietoturvaa nykyajan digitaalisessa maailmassa verrattuna muihin vastaaviin palveluntarjoajiin.

10.4 Jatkokehitysmahdollisuudet

Cisco Duoon pystytään tulevaisuudessa vielä lisätä ja ottaa käyttöön uusia ominaisuuksia sekä sitä voidaan laajentaa toimintaan suuremmalle joukolle Frendyn asiakkaista. Monet näistä ominaisuuksista edellyttävät suuresti työtä ja aikaa, joten ne eivät sopineet tähän käyttöönottoon. Toimeksiantajalla on tarkoituksena silti kehittää sekä laajentaa jatkossa toimintaa, ja olemmekin miettineet jo yhdessä erilaisia toimintoja, joita voitaisiin liittää Cisco Duoon.

Yksi oleellisimmista jatkokehitysmahdollisuuksista on AiTM-hyökkäyksen mahdollisuuden testaus ja sen tarkastelu, joka jouduttiinkin jättämään kesken rajallisen ajan takia jo suunnitteluvaiheessa. Testaus aloitettaisiin kuitenkin luomalla testiympäristön Microsoft Entra -vuokraajalle tarvittavan kokoinen virtuaalinen Ubuntu-tietokone, jonne eri vaiheiden jälkeen asennettaisiin ja konfiguroitaisiin Evilginx 3.0 -ohjelma käyttöön. Tämän jälkeen haettaisiin käyttövalmis Office 365:den kirjautumisnäkymän phislet ja konfiguroitaisiin se käyttöön, minkä avulla pystyttäisiin testaamaan AiTM-hyökkäystä Cisco Duo MFA:n kanssa. Frendyn on tarkoitus toteuttaa tämä jatkokehitysmahdollisuus myöhemmin lähitulevaisuudessa.

Mahdollisia muita jatkokehityksiä on Cisco Duon toiminnallisuuksien ja käytäntöjen yleisesti laajempi hyödyntäminen sekä muokkaaminen, kuten geofencing-ominaisuuksien käyttöönotto käyttäjien todentamisessa sijainnin perusteella, mikä voisi parantaa tietoturvan personointia ja tehokkuutta. Lisäksi voidaan tutkia koneoppimisen ja tekoälyn integrointia järjestelmään, jotta pystytään ennustaa ja tunnistaa epätyypillisiä kirjautumisyrityksiä entistä tarkemmin.

Jatkokehitysmahdollisuuksina voitaisiin harkita myös hajautetun ledger-teknologian, kuten blockchainin integrointia todentamisprosessiin, mikä lisäisi todentamistapahtumien läpinäkyvyyttä ja turvallisuutta. Lisäksi voitaisiin kehittää käyttäjien roolipohjaista todentamista, joka mukauttaa todentamisvaatimuksia käyttäjän roolin ja käyttöoikeuksien mukaan tehden järjestelmästä jousta-

vamman. Kolmas alue voisi olla virtuaalitodellisuuden tai lisätyn todellisuuden teknologioiden hyödyntäminen koulutustarkoituksiin tarjoten interaktiivisia oppimiskokemuksia tietoturvan parantamiseksi.

10.5 Opinnäytetyöprosessi

Opinnäytetyön prosessi oli monivaiheinen ja opettavainen matka, joka alkoi Cisco Duo MFA:n asennusprojektista Frendyn testiympäristössä. Tämä projekti tarjosi tilaisuuden soveltaa teoreettista tietämystä käytännön työtehtäviin ja kehittää ammatillisia taitoja IT-alalla.

Projektin toteutusvaihe oli yhteistyölähtöinen sisältäen keskusteluja ja muutamia palavereita toimeksiantajan tietoturvapuolen asiantuntijoiden kanssa. Tämä yhteistyö oli avainasemassa projektin onnistumiselle, ja se tarjosi minulle arvokasta näkemystä todellisen työelämän ongelmanratkaisuun ja päätöksentekoon. Erityisen hyödylliseksi osoittautui itsenäinen tutkimus ja testaus, mikä opetti paljon syvällisemmin työskentelyn kohteena olevista teknologioista ja niiden soveltamisesta. Testausvaihe toi esiin järjestelmän toimivuuden todellisissa käyttöolosuhteissa ja auttoi ymmärtämään, kuinka teoreettiset tietoturvaratkaisut toimivat käytännössä. Se opetti, miten tärkeää on jatkuva testaus ja sopeutuminen muuttuviin olosuhteisiin IT-projekteissa.

Microsoft Active Directoryn ja Microsoft Entran ID:n välinen synkronointi oli keskeinen osa projektia, joka mahdollisti identiteettien yhtenäisen hallinnan ja paransi tietoturvaa sekä käyttökokemusta. Tämä osa-alue korosti, kuinka tärkeää on ymmärtää ja hallita pilvipohjaisia palveluja yhdistettynä paikallisiin IT-infrastruktuureihin nykyaikaisessa tietotekniikassa. Duo Authentication Proxy -määrityksen toteutus ja Duo Securityn sekä Duo Mobilen käyttöönoton ymmärtäminen tarjosivat mahdollisuuden tutustua syvällisemmin monivaiheiseen todentamiseen ja sen tietoturvallisiin aspekteihin. Tämä osa opinnäytetyötäni korosti, miten tärkeää on ymmärtää monimutkaisten järjestelmien välisiä yhteyksiä ja niiden vaikutusta kokonaisvaltaiseen tietoturvaan.

Kokonaisuudessaan opinnäytetyöprosessi opetti paljon projektinhallinnasta, tietoturvasta ja siitä, kuinka tärkeää on yhdistää teoria ja käytäntö. Se oli haasteellinen ja pitkäjänteisyyttä vaativa, mutta samalla erittäin palkitseva kokemus, joka varmasti hyödyttää tulevaisuudessa IT-alan uralla. Opinnäytetyön aiheen löytäminen oli aluksi haastavaa, mutta onneksi Frendyn tarjoama apu osoittautui arvokkaaksi, ja heidän avullaan löysi sopivan aiheen. Tämän jälkeen koko prosessi aina työn

aloittamisesta sen viimeistelyyn saakka tuntui merkittävältä saavutukselta. Opinnäytetyön valmistuminen oli kuin voiton hetki, joka kruunasi työn ja vaivan, joka siihen oli panostettu.

Lähteet

Active Directory Domain Services Overview. 2022. Artikkeli Microsoft Learn -verkkosivustolla. Viitattu 24.11.2023. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview.

Active Directory Sync for Duo Users and Admins. 2023. Dokumentaatio Cisco Duo -verkkosivustolla. Viitattu 29.11.2023. https://duo.com/docs/adsync.

Adversary-in-the-Middle. 2023. Hyökkäystekniikka The MITRE Corporation -verkkosivustolla. Viitattu 10.11.2023. https://attack.mitre.org/techniques/T1557/.

Andreev, S., Bezzateev, S., Koucheryavy, Y., Mikkonen, T., Mäkitalo, N. & Ometov, A. 2018. Multi-Factor Authentication: A Survey. Avoin tutkimusartikkeli MDPI-verkkosivustolla. Viitattu 2.11.2023. https://doi.org/10.3390/cryptography2010001.

Authentication Methods: First Line of Defense. N.d. Tuote-esittely Cisco Duo -verkkosivustolla. Viitattu 25.10.2023. https://duo.com/product/multi-factor-authentication-mfa/authentication-methods.

Back to basics: Multi-factor authentication (MFA). 2023. Artikkeli NIST-verkkosivustolla. Viitattu 3.11.2023. https://www.nist.gov/itl/applied-cybersecurity/back-basics-multi-factor-authentication-mfa.

Boonkrong, S. 2021. Authentication and Access Control: Practical Cryptography Methods and Tools. Viitattu 2.11.2023. https://janet.finna.fi, Skillsoft Books ITPro (Skillport Platform).

Burr, W., Choong, Y., Danker, J., Fenton, J., Garcia, M., Grassi, P., Greene, K., Lefkovitz, N., Newton, E., Perlner, R., Regenscheid, A., Richer, J. & Theofanos, M. 2020. NIST Special Publication 800-63-3B: Digital Identity Guidelines. Dokumentti NIST-verkkosivustolla. Viitattu 27.10.2023. https://pages.nist.gov/800-63-3-Implementation-Resources/63B/Authenticators/.

Cisco Duo. N.d. Cisco Duo -kotisivut. Viitattu 24.11.2023. https://duo.com/.

Detecting and mitigating a multi-stage AiTM phishing and BEC campaign. 2023. Blogi Microsoft Security -verkkosivustolla. Viitattu 10.11.2023. https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/.

Duo Administration – Policy & Control. 2023. Dokumentaatio Cisco Duo -verkkosivustolla. Viitattu 8.11.2023. https://duo.com/docs/policy#verified-push.

Duo Administration - Protecting Applications. 2023. Dokumentaatio Cisco Duo -verkkosivustolla. Viitattu 22.11.2023. https://duo.com/docs/protecting-applications.

Duo Advantage. N.d. Version esittely Cisco Duo -verkkosivustolla. Viitattu 2.11.2023. https://duo.com/editions-and-pricing/duo-advantage.

Duo Authentication Proxy – Reference. 2023. Dokumentaatio Cisco Duo -verkkosivustolla. Viitattu 1.12.2023. https://duo.com/docs/authproxy-reference.

Duo Desktop. 2023. Dokumentaatio Cisco Duo -verkkosivustolla. Viitattu 10.11.2023. https://duo.com/docs/duo-desktop.

Duo Device Management Portal for End Users. 2023. Dokumentaatio Cisco Duo -verkkosivustolla. Viitattu 1.12.2023. https://duo.com/docs/device-management.

Duo Essentials. N.d. Version esittely Cisco Duo -verkkosivustolla. Viitattu 2.11.2023. https://duo.com/editions-and-pricing/duo-essentials.

Duo Free. N.d. Version esittely Cisco Duo -verkkosivustolla. Viitattu 2.11.2023. https://duo.com/editions-and-pricing/duo-free.

Duo Premier. N.d. Version esittely Cisco Duo -verkkosivustolla. Viitattu 2.11.2023. https://duo.com/editions-and-pricing/duo-premier.

Duo Trusted Endpoints. 2023. Dokumentaatio Cisco Duo -verkkosivustolla. Viitattu 15.11.2023. https://duo.com/docs/trusted-endpoints.

Duo Two-Factor Authentication for Microsoft Entra ID (formerly Azure Active Directory). 2023. Dokumentaatio Cisco Duo -verkkosivustolla. Viitattu 18.10.2023. https://duo.com/docs/azure-ca.

Editions & Pricing. N.d. Listaus versioista ja hinnoista Cisco Duo -verkkosivustolla. Viitattu 2.11.2023. https://duo.com/editions-and-pricing.

Evilginx 3.0. 2018. Evilginxin repositorio Github-verkkosivustolla. Viitattu 2.2.2024. https://github.com/kgretzky/evilginx2.

Golden, J. 2024. Understanding & Defending Against Adversary-in-the-Middle (AiTM) Attacks. Blogi Cisco Duo -verkkosivustolla. Viitattu 19.1.2024. https://duo.com/blog/understanding-defending-against-adversary-in-the-middle-aitm-attacks.

Grassi, P., Garcia, M. & Fenton, J. 2020. NIST Special Publication 800-63-3: Digital Identity Guidelines. Viitattu 27.10.2023. https://pages.nist.gov/800-63-3/sp800-63-3.html.

How it works: Microsoft Entra multifactor authentication. 2023. Artikkeli Microsoft Learn -verkkosivustolla. Viitattu 8.11.2023. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks.

Korppi, A. 2023. Tekninen arkkitehti tietoturva-puolelta. Frendy Oy. Sisäinen Teams-keskustelu 3.11.2023.

Karhula, T. 2023. Liiketoimintapäällikkö tietoturva-puolelta. Frendy Oy. Sisäinen Teams-keskustelu 3.11.2023.

LastPass MFA offers a passwordless experience for users. 2019. MFA ratkaisuesittely LastPass-verkkosivustolta ladattavassa pdf-dokumentissa. Viitattu 9.11.2023. https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LastPass-MFA-Overview-v2.pdf.

Microsoft Entra join a new Windows device during the out of box experience. 2023. Artikkeli Microsoft Learn -verkkosivustolla. Viitattu 1.12.2023. https://support.microsoft.com/en-us/account-billing/join-your-work-device-to-your-work-or-school-network-ef4d6adb-5095-4e51-829e-5457430f3973.

Morrow, S. 2020. 4 key problems with digital identity and why we need a new approach. Artikkeli CSO Online -verkkosivustolla. Viitattu 21.11.2023. https://www.csoonline.com/article/569089/4-key-problems-with-digital-identity-and-why-we-need-a-new-approach.html#:~:text=,more%20accurately%20and%20more%20safely.

Moving Beyond User Name & Pasword. N.d. Artikkeli Okta-verkkosivustolla. Viitattu 9.11.2023. https://www.okta.com/resources/whitepaper/adaptive.

How it works: Microsoft Entra multifactor authentication. 2023. Artikkeli Microsoft Learn -verkkosivustolla. Viitattu 1.12.2023. https://learn.microsoft.com/th-th/entra/identity/authentication/concept-authentication-methods.

LastPass MFA offers a passwordless experience for users. 2019. MFA ratkaisuesittely LastPass-verkkosivustolta ladattavassa pdf-dokumentissa. Viitattu 9.11.2023. https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LastPass-MFA-Overview-v2.pdf.

Multi-Factor Authentication (MFA). N.d. Tuote-esittely Cisco Duo -verkkosivustolla. Viitattu 25.10.2023. https://duo.com/product/multi-factor-authentication-mfa.

Multi-Factor Authentication. 2022. Ratkaisuesittely RSA-verkkosivustolta ladattavassa pdf-dokumentissa. Viitattu 9.11.2023. https://www.rsa.com/wp-content/uploads/multi-factor-authentication-rsa-sb.pdf.

Multi-Factor Authentication Interception. 2023. Hyökkäystekniikan esittely The MITRE Corporation -verkkosivustolla. Viitattu 10.11.2023. https://attack.mitre.org/techniques/T1111/.

MULTIFACTOR AUTHENTICATION INTEGRATIONS. N.d. Artikkeli LastPass-verkkosivustolla. Viitattu 9.11.2023. https://www.lastpass.com/solutions/integrations/mfa-integrations.

Not All MFA Solutions Are Created Equal. N.d. Artikkeli Cisco Duo -verkkosivustolla. Viitattu 10.11.2023. https://duo.com/why-duo/next-level-mfa.

One-Tap Authentication With Duo Push. N.d. Todennusmenetelmän esittely Cisco Duo -verkkosivustolla. Viitattu 8.11.2023. https://duo.com/product/multi-factor-authentication-mfa/authentication-methods/duo-push.

Remote Access Integrations. N.d. Tuote-esittely Cisco Duo -verkkosivustolla. Viitattu 25.10.2023. https://duo.com/product/remote-access/remote-access-integrations.

Sham, S. 2021. What Is Multi-Factor Authentication (MFA)?. Blogi Okta-verkkosivustolla. Viitattu 9.11.2023. https://www.okta.com/blog/2021/08/multi-factor-authentication-mfa/.

Two-Factor Authentication (2FA). N.d. Artikkeli Cisco Duo -verkkosivustolla. Viitattu 17.11.2023. https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa.

User Self-Service. N.d. Artikkeli Cisco Duo -verkkosivustolla. Viitattu 19.1.2024. https://duo.com/product/multi-factor-authentication-mfa/user-self-service.

WebAuthn: Biometrics and Security Keys. N.d. Todennusmenetelmän esittely Cisco Duo -verkkosivustolla. Viitattu 8.11.2023. https://duo.com/product/multi-factor-authentication-mfa/authentication-methods/biometrics-and-security-keys.

What is Microsoft Entra ID?. 2023. Artikkeli Microsoft Learn -verkkosivustolla. Viitattu 24.11.2023. https://learn.microsoft.com/en-us/entra/fundamentals/whatis.

What is Multi-Factor Authentication (MFA) and How does it Work?. 2021. Blogi RSA-verkkosivustolla. Viitattu 9.11.2023. https://www.rsa.com/multi-factor-authentication/what-is-mfa/.

What Is MFA?. N.d. Artikkeli Cisco Duo-verkkosivustolla. Viitattu 6.11.2023. https://duo.com/product/multi-factor-authentication-mfa/what-is-mfa.

Yasar, K. 2023. multifactor authentication. Määritelmä TechTarget-verkkosivustolla. Viitattu 31.10.2023. https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA.

Yritys. N.d. Frendy Oy -kotisivut. Viitattu 18.10.2023. https://frendy.fi/yritys.