jamk

Monivaiheisen tunnistautumisen käyttäjäystävällisyys

Laura Laitinen

Opinnäytetyö, AMK
Toukokuu 2024
Tieto- ja viestintätekniikan tutkinto-ohjelma

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Laitinen, Laura

Monivaiheisen tunnistautumisen käyttäjäystävällisyys

Jyväskylä: Jyväskylän ammattikorkeakoulu. **Toukokuu 2024**, 18 sivua.

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Monet tärkeät asiat hoidetaan nykyään internetin välityksellä, ja henkilökohtaisiin tietoihinsa pääsee käsiksi mistä tahansa ja milloin tahansa. Käyttäjän tunnistaminen on tärkeää, jotta arkaluontoiset tiedot eivät joudu vääriin käsiin. Perinteinen yksivaiheinen käyttäjätunnusta ja salasanaa hyödyntävä tunnistautumien ei aina riitä suojaamaan käyttäjätilejä, joten monet palvelut ovat siirtyneet monivaiheiseen tunnistautumiseen. Monivaiheisessa tunnistautumisessa käyttäjän tunnistamiseen käytetään vähintään kahta eri todennustekijää. Monivaiheisen tunnistautumisen haittapuolena on, että se on yksivaiheista tunnistautumista monimutkaisempi prosessi, mikä voi vaikuttaa negatiivisesti käyttäjäystävällisyyteen ja saavutettavuuteen.

Työ toteutettiin kuvailevana kirjallisuuskatsauksena. Tavoitteena oli selvittää, millaista tietoa monivaiheisen tunnistautumisen käyttäjäystävällisyydestä ja saavutettavuudesta löytyy, jäsennellä tietoa, sekä löytää aiheeseen uusia näkökulmia.

Työssä vertailtiin eri todennustekijöiden käyttäjäystävällisyyttä ja saavutettavuutta sekä tarkasteltiin yksilön saavutettavuustarpeisiin vaikuttavia seikkoja. Todennustekijöiden välillä on eroja ja käyttäjän tarpeet vaikuttavat siihen, mikä juuri hänelle sopii parhaiten. Saavutettavuustarpeisiin vaikuttavia yksilön ominaisuuksien selvitettiin olevan kognitiiviset kyvyt, näkö, kuulo, elintoiminnot sekä motoriset kyvyt.

Käytettyjen lähteiden perusteella päädyttiin johtopäätöksiin siitä, millaiset seikat tekevät tunnistautumisprosessista käyttäjäystävällisen ja saavutettavan. Käyttäjäystävällisen prosessin ominaisuuksien pääteltiin olevan mukautuvuus yksilön tarpeisiin, tunnistautumisen sujuvuus sekä käyttäjän motivoiminen vahvemman tunnistautumisen käyttöön. Saavutettavan prosessin ominaisuuksien puolestaan pääteltiin olevan mukautuminen yksilön tarpeisiin, tunnistautumisen sujuvuus sekä käytön kuormittavuus.

Avainsanat (asiasanat)

MFA, 2FA, monivaiheinen tunnistautuminen, käyttäjäystävällisyys, saavutettavuus

Muut tiedot (salassa pidettävät liitteet)

-

jamk

Description

Laitinen, Laura

Usability of Multi-Factor Authentication

Jyväskylä: JAMK University of Applied Sciences, May 2024, 18 pages.

Degree Programme in Information and Communications technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

Today many important matters are handled online, and users can access their personal information from any location at any given time. Identifying the user is important to avoid situations where their personal information ends up in the wrong hands. Traditional single-factor authentication that only requires a combination of a username and password is not always enough to protect user accounts, so many platforms have opted for multi-factor authentication. Multi-factor authentication uses a minimum of two authentication factors to identify users. Multi-factor authentication is intrinsically more complicated than single-factor authentication, which may have a negative effect on usability and accessibility.

The thesis was conducted as a narrative literature review. The aim was to discover what kind of information regarding the usability and accessibility of multifactor authentication is already available, organize existing information, and find new perspectives regarding the topic.

Different authentication factors were compared based on their usability and accessibility. The aspects which affect individuals' accessibility needs were also examined. There are a range of different authentication factors, and their level of usability and accessibility depends on the user's abilities. Cognitive abilities, sight, hearing, some life functions, and motoric skills have an impact on the accessibility needs of individuals.

Based on the source material it was concluded that a usable authentication method consists of adaptability to users' needs, conveniency of the process and motivating the user to adopt multi-factor authentication. Accessible authentication was concluded to consist of adaptability to users' needs, conveniency of the process and effortlessness.

Keywords/tags (subjects)

MFA, 2FA, multi-factor authentication, usability, accessibility

Miscellaneous (Confidential information)

-

Sisältö

1 Johdanto

Laskujen maksaminen, terveystietojen tarkastelu ja ostosten tekeminen hoituvat nykyään internetin välityksellä, mikä on kätevää. Aikaa ja vaivaa säästyy, kun asioiden hoitaminen onnistuu kotoa käsin. Se, että jokainen pääsee käsiksi henkilökohtaisiin tietoihinsa sijainnista ja kellonajasta riippumatta tarkoittaa kuitenkin, että myös rikolliset voivat päästä käsiksi näihin samoihin tietoihin mistä tahansa. Tämän vuoksi käyttäjän henkilöllisyyden varmistaminen on nykyään erityisen tärkeää.

Koska monet tärkeät ja pakolliset asiat hoidetaan verkossa, on tärkeää, että palvelut on suunniteltu niin, että ne ottavat huomioon käyttäjien erilaiset tarpeet, ja mahdollistavat palvelun sujuvan käyttämisen kaikille. Nykytilanne on se, että monet käyttäjät kokevat monivaiheisen tunnistautumisen työlääksi, liian monimutkaiseksi tai täysin turhaksi (Camp, Das & Wang 2019). Joillekin käyttäjille tunnistautumisprosessi on kohtuuttoman työläs, johtuen siitä, ettei se ota tarpeeksi hyvin huomioon käyttäjien välisiä eroja saavutettavuustarpeiden suhteen.

Tämän opinnäytetyön tavoitteena oli tarkastella monivaiheista tunnistautumista käyttäjäystävällisyyden ja saavutettavuuden näkökulmasta. Käyttäjäystävällisyydellä tai käytettävyydellä tarkoitetaan järjestelmän soveltuvuutta suunniteltuun tarkoitukseen tietylle kohderyhmälle (TEPA-termipankki, 2002). Saavutettavuudella puolestaan tarkoitetaan ihmisten erilaisten kykyjen ja tarpeiden huomiointia palvelun toteuttamisessa (Yleistä saavutettavuudesta, n.d.).

Saavutettavuus ja käyttäjäystävällisyys ovat olennaisia asioita kaiken digitaalisen sisällön suhteen, mutta monia palveluita ei voi käyttää, ellei ensin tunnistaudu. Palvelun saavutettavuudella ei ole merkitystä, jos tunnistautumisprosessin puutteet estävät käyttäjää pääsemästä käsiksi palveluun. Monivaiheisen tunnistautumisen ollessa vapaaehtoista sen saavutettavuuspuutteet ja huono käyttäjäkokemus nostavat todennäköisyyttä sille, että käyttäjät jatkavat perinteisen yksivaiheisen tunnistautumisen käyttöä, mikä laskee palvelun tietoturvaa. Nämä seikat vaikuttivat siihen, että valitsin tutkimuskohteeksi juuri monivaiheisen tunnistautumisen käyttäjäystävällisyyden.

2 Tutkimusasetelma

2.1 Tutkimuskysymykset

Opinnäytetyön tavoitteena on vastata seuraaviin tutkimuskysymyksiin:

1. Mikä tekee monivaiheisesta tunnistautumisprosessista käyttäjäystävällisen?
2. Mikä tekee monivaiheisesta tunnistautumisprosessista saavutettavan?
3. Miten käyttäjäystävällisyyden ja saavutettavuuden vaatimukset voidaan saavuttaa?

2.2 Tutkimusmenetelmä

Tämän opinnäytetyön tutkimusmenetelmäksi valikoitui kuvaileva kirjallisuuskatsaus, koska halusin selvittää, millaista tietoa aiheesta jo löytyy sekä ymmärtää monivaiheisen tunnistautumisen luomia saavutettavuushaasteita. Halusin myös jäsennellä jo olemassa olevia ratkaisuja näihin haasteisiin ja mahdollisesti löytää uusia näkökulmia epäkohtien korjaamisen suhteen.

Kirjallisuuskatsaus yhdistelee järjestelmällistä tutkimusten hakuprosessia, tutkimusten valikointia, löydettyjen tutkimusten kriittistä lukemista ja arviointia, muistiinpanojen tekemistä alkuperäistutkimuksista, tutkimusten analyysia sekä tietojen yhdistämistä uuden tiedon tuottamiseksi. Kirjallisuuskatsauksen tavoitteena on kuvata, mitä aiheesta jo tiedetään sekä löytää uusia tutkimuskysymyksiä ja näkökulmia. (Vilkka 2023, 14.)

3 Monivaiheinen tunnistautuminen

3.1 Yleistä

Monivaiheinen tunnistautuminen (Multi-factor Authentication, MFA) on prosessi, jossa käyttäjän henkilöllisyys varmistetaan käyttämällä vähintään kahta eri tunnistautumistapaa. Yleisin monivaiheisen tunnistautumisen muoto on kaksivaiheinen tunnistautuminen (Two-factor Authentication, 2FA). Monivaiheinen tunnistautuminen edellyttää, että käyttäjällä on ainakin kaksi seuraavista:

1. Jotakin, mitä hän tietää (esimerkiksi salasana)
2. Jotakin, jota hänellä on (esimerkiksi matkapuhelimeen tekstiviestillä lähetettävä koodi)
3. Jotakin, jota hän on (biometrinen tunnistautuminen, esimerkiksi sormenjälki- tai kasvotunnistus) (Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi, 2023.)

Monivaiheinen tunnistautuminen tarjoaa yksivaiheista tunnistautumista huomattavasti paremman tietoturvan, sillä yleisimmät syyt käyttäjätilin kaapatuksi tulemiselle ovat heikko salasana tai saman salasanan käyttäminen useilla eri alustoilla. Monivaiheinen tunnistautuminen on tällä hetkellä paras tapa suojata käyttäjätilejä luvattomalta käytöltä. (Multifactor Authentication Cheat Sheet n.d.)

3.2 Todennustekijät

Käyttäjä voi usein valita muutamien eri todennustekijöiden välillä, tai halutessaan ottaa käyttöön useamman eri menetelmän. Usean todennustekijän käyttöönotto voi helpottaa tunnistautumista esimerkiksi puhelimen mennessä rikki.

3.3 Biometriset todennustekijät

Biometriset todennustekijät perustuvat johonkin käyttäjän fyysiseen ominaisuuteen. Sormenjälkitunnistautuminen ja kasvojentunnistus ovat nykypäivänä arkipäivää useimmille älypuhelimen käyttäjille. Muita biometriseen tunnistautumiseen hyödynnettäviä tekijöitä ovat mm. puheääni, silmän iiris tai verisuonten sijainti. (Kinzer 2022.)

Biometriset tekijät ovat synnynnäinen osa käyttäjää, joten ne kulkevat aina mukana, ja niiden väärentäminen on vaikeaa. Biometrisen tunnistautumisen käyttäminen on usein helppoa, eikä vaadi käyttäjää suorittamaan monimutkaisia toimintoja tai siirtymään toiseen sovellukseen. Biometrisessä tunnistautumisessa on kuitenkin myös ongelmakohtia. Koska biometriset tekijät ovat melko pysyvä ja olennainen osa käyttäjää itseään, on niihin liittyvän datan joutuminen vääriin käsiin ongelmallista. Murretun salasanan voi vaihtaa suhteellisen helposti, kasvojen rakennetta tai sormenjälkeä ei. Esimerkiksi GDPR määrittelee biometrisen datan kuuluvan erityisiin henkilötietoryhmiin, joita on suojeltava erittäin tarkasti (GDPR 2016/679)

Toinen biometriseen tunnistautumiseen liittyvä epäkohta on biometrisen tunnistautumisen tarkkuuden vaihtelu eri käyttäjäryhmien välillä. Erään tutkimuksen mukaan kasvojentunnistusalgorit-

mit tuottavat eniten vääriä positiivisia tuloksia länsiafrikkalaisessa, itäafrikkalaisessa ja itäaasialaisessa väestössä. Vähiten vääriä positiivisia tuloksia ilmeni itäeurooppalaisen väestön edustajilla. Etnisyyden lisäksi tulosten tarkkuuteen vaikuttavat myös käyttäjän ikä ja sukupuoli. Yksi oleellisimmista tulosten tarkkuutta lisäävistä keinoista on algoritmin kouluttamiseen käytetyn aineiston suurempi monipuolisuus. (Grother, Hanaoka & Ngan 2019.)

3.4 Kertakäyttöinen aikaan perustuva salasana (TOTP)

Kertakäyttöinen aikaan perustuva salasana (Time-based One-Time Password, TOTP) on kertakäyttöinen satunnaisgeneroitu koodi, joka on voimassa vain hetken. RFC6238-standardissa TOTP-koodin voimassaoloajaksi suositellaan 30 sekuntia. Liian pieni voimassaoloaika ei anna käyttäjälle tarpeeksi aikaa koodin syöttämiseen. Liian pitkästä voimassaoloajasta taas kärsivät sekä tietoturva, että käyttäjäystävällisyys. Mitä pidempään koodi on voimassa, sitä suurempi aikaikkuna hyökkääjillä on käytettävänään. Pidempi voimassaoloaika tarkoittaa myös, että seuraavan koodin generoitumiseen kuluva aika on pidempi, mikä on ongelmallista, jos käyttäjä tarvitsee uuden koodin. (Machani, M'Raihi, Pei & Rydell 2011.)

Käyttäjäystävällisyyden näkökulmasta tarkasteltuna TOTP vaatii käyttäjältä hieman enemmän kuin biometriset todennustekijät. Useimmiten käyttäjä vastaanottaa TOTP-koodin puhelimeensa joko erilliseen todentajasovellukseen tai tekstiviestinä. Käyttäjän on pystyttävä avaamaan erillinen sovellus, lukemaan koodi ja syöttämään se tunnistautumista vaativaan palveluun. Prosessi voi olla vaikeampi käyttäjille, joilla on puutteita näkökyvyssä, kognitiossa tai motoriikassa.

3.5 Tekstiviestit

Tekstiviestin avustuksella tapahtuvassa tunnistautumisessa käyttäjän puhelimeen lähetetään tunnistautumiskoodin sisältävä tekstiviesti. Tekstiviestitunnistautuminen vaatii käyttäjältä samanlaisia toimintoja kuin TOTP-koodin käyttäminen, mutta se ei vaadi erillisen tunnistautumissovelluksen asentamista.

TOTP-todennukseen verrattuna tekstiviestitunnistautumisen tietoturva on heikompi, koska koodi generoidaan laitteen ulkopuolella ja lähetetään käyttäjälle matkapuhelinverkon kautta. Hyökkääjät

voivat esimerkiksi kaapata SIM-kortin (sim swapping) tai hyväksikäyttää viestien välittämiseen käytetyn SS7-protokollan haavoittuvuuksia. (Augoye 2023.)

3.6 Push-ilmoitukset

Push-ilmoitukset ovat puhelimen tai tietokoneen näytölle ilmestyviä lyhyitä viesti-ikkunoita, jotka voivat sisältää tekstiä tai interaktiivista mediaa, kuten kuvia tai painettavia näppäimiä, jotka suorittavat jonkin toiminnon (What is a push notification n.d.). Tunnistautumisprosessissa käyttäjän älypuhelimeen lähetetään push-ilmoitus, joka sisältää painikkeen, jota painamalla käyttäjä voi hyväksyä kirjautumisyrityksen. Käyttäjän ei siis tarvitse avata erillistä sovellusta tai syöttää tekstiä. Push-ilmoitukset voivat paremman tarjota vaihtoehdon käyttäjille, joilla on vaikeuksia esimerkiksi TOTP-koodin syöttämisessä sen lyhyen aikaikkunan sisällä. (Lake 2021.)

Push-ilmoituksen käyttäminen on nopeaa ja yksinkertaista, mutta se on muita todennusmenetelmiä alttiimpi väsytyshyökkäykselle (MFA fatigue attack). Käyttäjän käyttäjätunnuksen ja salasanan ollessa hyökkääjän hallussa hän voi suorittaa useita kirjautumisyrityksiä, minkä seurauksena käyttäjä saa lukuisia tunnistautumispyyntöjä. Tavoitteena on saada käyttäjä epähuomiossa hyväksymään kirjautumisyritys. (Abrams 2022.) Tämän takia esimerkiksi Microsoft lisäsi toukokuussa 2023 tunnistautumissovelluksensa push-ilmoituksiin pakollisen lisävaiheen, jossa käyttäjää pyydetään syöttämään sovellukseen kirjautumissivulla näkyvä kaksinumeroinen luku (Authentication Documentation 2023).

3.7 Todennuslaite

Todennuslaite on fyysinen laite, jota voidaan käyttää todennustekijänä. Todennuslaitteita on erilaisia. Osa laitteista hyödyntää Bluetooth- tai NFC-teknologiaa mahdollistaakseen kontaktittoman tunnistautumisen. Jotkin laitteet puolestaan kytketään esimerkiksi tietokoneen USB-porttiin. Joitakin fyysisiä todennuslaitteita ei kytketä toiseen laitteeseen, vaan ne generoivat koodin, jonka käyttäjä syöttää tunnistautumista vaativaan palveluun. Tunnistautumissovelluksella varustettu älypuhelin voidaan luokitella fyysiseksi todennuslaitteeksi. (What Is a Security Token 2023.)

Todennuslaitteen käyttäjäystävällisyys ja saavutettavuus riippuvat sen ominaisuuksista. TOTP-koodeja generoivat laitteet ovat käyttäjäkokemukseltaan melko samankaltaisia puhelimeen ladattavien tunnistautumissovellusten kanssa. USB-porttiin kytkettävät ja langatonta teknologiaa hyödyntävät todennuslaitteet sen sijaan poistavat tarpeen erillisen koodin lukemiselle ja syöttämiselle, mikä voi tehdä tunnistautumisprosessista saavutettavamman käyttäjille, joilla on puutteita näkökyvyssä, kognitiossa tai motorisissa taidoissa. (Lake 2021.)

4 Yksilön saavutettavuusvaatimuksiin vaikuttavat tekijät

4.1 Saavutettavuustarpeiden määrittely

Maailman terveysjärjestö WHO:n ICF-luokitus kuvaa yksilön toimintakykyä, toimintarajoitteita ja terveyttä, sekä sairauden tai vamman vaikutuksia yksilön elämässä (ICF-luokitus 2024). Furnell, Helkala ja Woods (2022) tarkastelivat ICF-luokitusta määritelläkseen yksilön ominaisuuksia, jotka vaikuttavat käyttäjän saavutettavuustarpeisiin tunnistautumisprosessin suhteen. Heidän mukaansa tällaisia ominaisuuksia ovat älylliset kyvyt, keskittymiskyky, muisti, visuaalinen havainnointi, kuulo, kyky oppia lukemaan, kirjoittamaan ja laskemaan, elintoiminnot, puhe, hienomotoriset kyvyt sekä kävelykyky. (Furnell, Helkala & Woods 2022.)

4.2 Kognitiiviset kyvyt

Kognitiivisilla kyvyillä tarkoitetaan tiedon käsittelyyn liittyviä toimintoja kuten havaitsemista, ajattelua ja muistamista (Vuoksimaa 2019). Kognitiivisiin kykyihin vaikuttavat mm. ikääntyminen, muistisairaudet, kehitysvammat, mielenterveysongelmat ja neuropsykiatriset häiriöt.

Yleensä monivaiheinen tunnistautuminen vaatii käyttäjältä usean toiminnon suorittamista oikeassa järjestyksessä tietyn ajan sisällä. Tämä on totta etenkin TOTP-koodia käytettäessä. Biometriset todennustekijät taas eivät yleensä vaadi käyttäjältä muuta kuin esimerkiksi sormen tai kasvojen asettamisen oikeaan kohtaan, joten se voi olla parempi vaihtoehto käyttäjille, joilla on vaikeuksia kognitiivisten toimintojen kanssa.

4.3 Näkökyky

Näkövammainen henkilö voi olla heikkonäköinen tai sokea. Henkilöä voidaan pitää sokeana, jos hän ei pysty liikkumaan näön perusteella tuntemattomassa paikassa. Suuri osa näkövammaisista on ikääntyneitä, koska monet näkövamman taustalla olevat sairaudet ovat yhteydessä ikääntymiseen. (Näkövammaisuus 2022)

Monet todennustekijät hyödyntävät käyttäjän näköaistia. TOTP-sovellukset vaativat käyttäjää lukemaan koodin ja syöttämään sen tunnistautumista vaativaan palveluun. Myös fyysisten todennuslaitteiden käyttö voi olla työläämpää näkövammaiselle, jos laite täytyy kytkeä esimerkiksi toisessa laitteessa olevaan USB-porttiin. Biometriset todennustekijät voivat olla näkövammaisille muita tunnistautumiskeinoja helppokäyttöisempiä. Poikkeuksena tähän on kuitenkin silmän iiriksen kuvioinnin tunnistamista hyödyntävä biometrinen tunnistautuminen, koska jotkin sairaudet, esimerkiksi harmaakaihi, muuttavat silmän ulkonäköä (Czajka, Maciejewicz & Trokielewicz 2019).

4.4 Kuulo

Kuulovammaisella henkilöllä on jonkinasteinen tai -laatuinen kuulonalenema, joka voi vaihdella lievästä huonokuuloisuudesta täydelliseen kuurouteen. Kuulonaleneman voivat aiheuttaa esimerkiksi korvan, kuulohermon ja keskushermoston vauriot. (Kuulovammat n.d.)

Suurin osa todennustekijöistä ja tunnistautumisjärjestelmistä ei hyödynnä käyttäjän kuuloaistia. Kuulon alenema voi kuitenkin aiheuttaa vaikeuksia tunnistautumisessa, etenkin jos käyttäjällä on sen lisäksi muitakin rajoitteita, kuten näkövamma. Tässä tilanteessa näkövammaisille suunnatut kuuloaistiin perustuvat tunnistautumistavat eivät välttämättä ole hyödyllisiä.

4.5 Elintoiminnot

Joidenkin elintoimintojen häiriöt ja muutokset voivat haitata biometristen todennustekijöiden käyttöä. Esimerkkinä tästä on aiemmin mainittu silmäsairauksien vaikutus iiristunnistautumiseen (Czajka, Maciejewicz & Trokielewicz 2019). Ihon vauriot tai muutokset puolestaan voivat muuttaa ihon ulkonäköä ja vaikeuttaa sormenjälkien tai kasvojen tunnistusta (Brezinova, Dolezel, Drahansky & Urbanek 2012).

4.6 Motoriset kyvyt

Motoriset kyvyt voidaan jakaa hienomotorisiin ja karkeamotorisiin. Hienomotorisilla taidoilla tarkoitetaan pienillä lihaksilla suoritettavia tarkkuutta vaativia liikkeitä. Karkeamotorisilla taidoilla puolestaan viitataan suurilla lihasryhmillä suoritettavia liikkeitä. (Motoriset taidot – mitä ne ovat n.d.)

Useimpien tunnistautumistapojen käyttöön tarvitaan jonkinlaisia hienomotorisia taitoja. Esimerkiksi tunnistussovelluksen käyttö vaatii useita hienomotoriikkaa hyödyntäviä toimintoja, kuten hiiren käyttäminen, kirjoittaminen tai kosketusnäytön käyttö. Karkeamotorisia taitoja hyödynnetään tunnistautumisessa harvemmin, mutta ne voivat vaikuttaa esimerkiksi käyttäjän kävelytyylin analysoimiseen perustuviin tunnistautumismenetelmiin.

5 Monivaiheisen tunnistautumisen ongelmat

5.1 Käyttäjäystävällisyyden puutteet

Camp, Das ja Wang (2019) perehtyivät eri MFA-sovellusten käyttäjäarvosteluihin ja määrittelivät kolme suurinta käyttäjien kokemaa ongelmaa. Ensimmäinen ongelma on varmuuskopioinnin ja laitteesta toiseen siirtymisen vaikeus. Toinen ongelma on käyttöönoton vaikeus ja yhteensopivuusongelmat. Käyttäjät haluavat tunnistautumissovellusten olevan yhteensopivia puhelimen lisäksi esimerkiksi älykellojen kanssa. Kolmas ongelma on käytön pakollisuus. Käyttäjät kertoivat työnantajan tai oppilaitoksen pakottavan heidät käyttämään monivaiheista tunnistautumista ilman perusteluja.

Monivaiheisen tunnistautumisen siirtäminen uuteen laitteeseen voi olla työlästä, varsinkin jos edellinen laite on hävinnyt, tullut varastetuksi tai mennyt rikki. Microsoft Authenticator - sovelluksessa uuden laitteen käyttöönotto onnistuu helpoiten palauttamalla edellisen varmuuskopion. Varmuuskopiointi ei kuitenkaan oletusarvoisesti ole päällä, vaan käyttäjän on aktivoitava se erikseen. Varmuuskopioinnin aktivointia varten käyttäjän on myös kirjauduttava sisään Microsoft-tilillä, joka ei kuitenkaan saa olla yksi sovelluksen tunnistautumisominaisuutta hyödyntävistä tileistä. (Back up and recover account credentials in the Authenticator app, n.d.) Ohjeet varmuuskopioinnin aktivointiin ja tunnistautumissovelluksen tietojen palauttamiseen löytyvät Google-haun avulla

nopeasti Microsoftin viralliselta tukisivustolta (support.microsoft.com). Englanninkieliset ohjeet ovat melko selkeät, mutta halutessaan ohjeita suomeksi joutuu käyttäjä tyytymään kehnoon käännökseen. Tämä vaikeuttaa prosessia käyttäjille, joiden englannin kielen taidossa on puutteita, tai joilla on muuten vaikeuksia seurata kirjallisia ohjeita. Puutteelliset IT-taidot yhdistettynä epäselviin ohjeisiin voivat tehdä prosessista käyttäjälle lähes mahdottoman ilman ulkopuolista apua.

Varmuuskopioinnin ja tunnistautumistietojen palauttamisen lisäksi myös monivaiheisen tunnistautumisen ottaminen käyttöön ensimmäistä kertaa voi tuottaa käyttäjille vaikeuksia. Esimerkiksi erilaiset oppimistavat, aiemmin hankitut ICT-taidot ja erot motivaatiossa vaikuttavat siihen, miten helppoa tai vaikeaa uuden järjestelmän käyttöönotto on. Myös käyttäjän kielitaidolla on merkitystä, sillä suurin osa netistä löytyvistä ohjeista on englanninkielisiä.

Kolmas käyttäjäkokemukseen vaikuttava ongelma on käytön pakollisuus. Monivaiheisen tunnistautumisen tekemisellä pakolliseksi vältetään heikon tunnistautumisen tietoturvauhat. Toisaalta osa käyttäjistä voi silloin välttää palvelun käyttämistä kokonaan. Yritysten sisällä tämä voi johtaa ns. varjo-IT:n käyttöön työntekijöiden keskuudessa. Varjo-IT:llä (shadow IT) tarkoitetaan ohjelmia, laitteita tai muita järjestelmiä, joita organisaation IT-osasto ei ole hyväksynyt. Tällaisten järjestelmien käyttö luo tietoturvariskejä ja lisää tietovuotojen todennäköisyyttä. (What is shadow IT n.d.)

5.2 Saavutettavuuden puutteet

Saavutettavuuden suhteen monivaiheisen tunnistautumisen ongelmia voi tarkastella esimerkiksi teknisen saavutettavuuden, helppokäyttöisyyden ja ymmärrettävyyden näkökulmista (Yleistä saavutettavuudesta n.d.). Saavutettavuuden ollessa puutteellista ihmisten erilaisuutta ei ole otettu huomioon, jolloin palvelun käyttäminen voi olla osalle käyttäjistä kohtuuttoman vaikeaa tai jopa mahdotonta.

Teknisellä saavutettavuudella viitataan palvelun tekniseen toteutukseen liittyviä seikkoja, kuten standardien ja saavutettavuusohjeistusten noudattamista ja palvelun yhteensopivuutta erilaisten päätelaitteiden ja avustavien teknologioiden kanssa (Yleistä saavutettavuudesta n.d.). Esimerkiksi Microsoft Authenticator ja Duo Mobile -tunnistautumissovellusten saavutettavuusraporttien perusteella sovellusten yhteensopivuudessa näytönlukijoiden kanssa on ongelmia (Cisco Accessibility Conformance Report 2023; Microsoft Accessibility Conformance Report 2023).

Helppokäyttöisyydellä tarkoitetaan palvelun hahmottamisen ja navigaation vaivattomuutta. Helppokäyttöisessä palvelussa sisältö on helppo hahmottaa ja halutun toiminnon suorittaminen onnistuu vaivattomasti. (Yleistä saavutettavuudesta n.d.) Vaikeakäyttöisessä palvelussa olennaisen sisällön hahmottaminen on vaikeaa ja toimintojen suorittaminen voi olla monimutkaista ja hidasta.

Ymmärrettävyydellä tarkoitetaan palvelun sisällön ymmärrettävyyttä kaikille käyttäjille. Tekstin tulisi olla helppolukuista ja hyvin jäsenneltyä. Ymmärrettävyyteen sisältyy myös sisällön tarjoaminen tekstin lisäksi videoina, kuvina ja ääninä. (Yleistä saavutettavuudesta n.d.) Huono ymmärrettävyys ilmenee vaikealukuisena ja sekavana tekstinä sekä vaihtoehtoisten sisältömuotojen puutteena.

5.3 Tietoturva

Vaikka monivaiheinen tunnistautuminen lisää tietoturvaa huomattavasti verrattuna perinteiseen yksivaiheiseen käyttäjänimeä ja salasanaa hyödyntävään tunnistautumiseen, on siinäkin omat tietoturva-aukkonsa. Etenkin tekstiviestitse lähetettäviä koodeja hyödyntävät tunnistautumistavat ovat saaneet osakseen kritiikkiä. Tekstiviestitunnistautuminen on altis esimerkiksi SIM swapping -hyökkäykselle, jossa ulkopuolinen henkilö teeskentelee liittymän omistajaa ja saa palveluntarjoajan yhdistämään liittymän uuteen SIM-korttiin. Mikäli tämä onnistuu, ohjautuvat uhrin tekstiviestit ja puhelut hyökkääjän hallussa olevaan SIM-korttiin, jolloin hän saa haltuunsa myös tunnistautumiseen käytetyt tekstiviestikoodit. (Molinaro 2023.)

Toinen merkittävä monivaiheiseen tunnistautumiseen liittyvä tietoturvauhka on väsytyshyökkäys (MFA fatigue attack), joka kohdistuu push-ilmoituksia hyödyntävään tunnistautumiseen. Väsytyshyökkäyksessä hyökkääjä yrittää kirjautua palveluun useita kertoja uhrin käyttäjätunnuksen ja salasanan avulla, jolloin uhri saa useita vahvistamista pyytäviä push-ilmoituksia. Tavoitteena on saada uhri väsymään jatkuviin ilmoituksiin, jolloin hän saattaa hyväksyä kirjautumisyrityksen pysäyttääkseen ilmoitustulvan. (Abrams 2022.)

6 Monivaiheisen tunnistautumisen kehittäminen

6.1 Palveluiden saavutettavuuden ja käyttäjäystävällisyyden tason selvittäminen

Palvelun saavutettavuutta ja käyttäjäystävällisyyttä voidaan arvioida testaamalla palvelun teknistä toteutusta, kuten sisällön värikontrastia, valikoiden näkyvyyttä ja aikaa, jonka käyttäjien suorittamat toiminnot vievät tai keräämällä kvalitatiivista tietoa käyttäjien kokemuksista kyselyiden ja palautteen muodossa (What is Usability Evaluation? 2016).

Palveluiden saavutettavuuden ja käyttäjäystävällisyyden tason selvittämiseen on olemassa erilaisia työkaluja, jotka voivat auttaa sekä manuaalisessa että automatisoidussa testauksessa. Mikään työkalu ei kuitenkaan voi yksinään määritellä saavutettavuuden ja käyttäjäystävällisyyden tasoa, vaan se tarvitsee rinnalleen ihmisen arviointikykyä. (Selecting Web Accessibility Evaluation Tools, 2023.)

System Usability Scale (SUS) on yksinkertainen kyselylomake, joka sisältää kymmenen väittämää, joihin käyttäjä vastaa asteikolla yhdestä viiteen, missä numero yksi tarkoittaa ”vahvasti eri mieltä” ja numero 5 tarkoittaa ”vahvasti samaa mieltä”. Alun perin John Brooke kehitti sen vuonna 1986 osana Digital Equipment Co Ltd:n sisäisten järjestelmien käyttäjäystävällisyyden arviointia varten, ja se on edelleen laajasti käytetty. (Soegaard, M. 2023.)

Käyttäjäystävällisyyden arviointiin tarkoitettuja kvalitatiivista tietoa kerääviä työkaluja voidaan usein optimoida niin, että niitä voidaan käyttää myös saavutettavuuden arvioimiseen. Saavutettavuuden arvioinnissa tulee keskittyä yleisen käyttäjätyytyväisyyden sijaan nimenomaan käyttöä estäviin tai vaikeuttaviin saavutettavuuteen liittyviin ongelmiin. Varsinaisten saavutettavuusongelmien lisäksi kuitenkin myös saavutettavuusominaisuuksia tarvitsevien käyttäjien kokemaan tyytyväisyyteen palvelun käytön suhteen tulee kiinnittää huomiota. (Involving Users in Evaluating Web Accessibility 2021.)

6.2 Palveluiden saavutettavan toteuttamisen takaaminen

Saavutettavuuden implementoinnin helpottamiseksi yhtenäiset ohjeet ja standardit ovat tarpeen. Lainsäädännön avulla puolestaan voidaan ainakin teoriassa varmistaa, että palveluntarjoajat toteuttavat näitä ohjeita ja standardeja. Lainsäädännön noudattamista tulisi myös pystyä valvomaan

jollakin tapaa. Suomessa käyttäjä voi tehdä aluehallintovirastolle kantelun palvelusta, joka ei noudata nykyisen digipalvelulain saavutettavuusvaatimuksia (Digipalvelulain vaatimukset n.d.).

Palveluiden saavutettavaa suunnittelua ohjaavat esimerkiksi Centre for Excellence in Universal Desig -organisaation Universal Design -periaatteet sekä W3C-organisaation Web Content Accessibility Guidelines (WCAG). Universal Design sisältää seitsemän saavutettavuuteen liittyvää periaatetta. Sen ydinajatus on, että jokainen ympäristö tulisi suunnitella siten, että se täyttää kaikkien sen käyttäjien tarpeet. Universal Design -periaatteita voidaan soveltaa IT-järjestelmien lisäksi myös fyysisiin rakennuksiin ja tuotteisiin. (About Universal Design n.d.) WCAG puolestaan keskittyy pelkästään verkkosisältöön. Sen tavoitteena on tehdä verkkosisällöstä saavutettavaa käyttäjille, joilla on erityisiä saavutettavuustarpeita. (Web Content Accessibility Guidelines 2023.) Se on sisällöltään Universal Design -ohjeistusta tarkempi ja yksityiskohtaisempi.

Esimerkkinä saavutettavuuden edistämisestä lainsäädännön avulla on vuonna 2019 Suomessa voimaan tullut digipalvelulaki, jonka tarkoituksena on edistää digitaalisten palveluiden saatavuutta, laatua ja tietoturvallisuutta. Lain voimaantuloon vaikuttivat Euroopan unionin saavutettavuus- ja esteettömyysdirektiivit sekä YK:n yleissopimus vammaisten henkilöiden oikeuksista. Lain vaatimukset koskevat julkista sektoria ja joitakin yksityisen ja kolmannen sektorin organisaatioita. Laki vaikuttaa moniin verkkosivustojen ja mobiilisovellusten sisältöihin ja toiminnallisuuksiin, mm. tekstit, kuvat, interaktiiviset grafiikat, videot sekä sivustolle upotetut chat-palvelut.

Digipalvelulain kolme keskeisintä vaatimusta ovat seuraavat:
1. Digitaalisen palvelun ja sisällön tulee täyttää eurooppalaisen standardin EN 301 549 määrittelemät tekniset vaatimukset.
2. Digitaalisesta palvelusta tulee löytyä saavutettavuusselosta, joka kertoo käyttäjille palvelun saavutettavuudesta.
3. Käyttäjällä tulee olla mahdollisuus antaa toimijalle palautetta saavutettavuudesta. Palautteeseen täytyy vastata 14 vuorokauden kuluessa. (Digipalvelulain vaatimukset n.d.)

6.3 Tekniset ratkaisut

Yksi monivaiheisen tunnistautumisen ongelmista on, että käyttäjä joutuu tunnistautumaan useisiin eri palveluihin, mikä vie aikaa ja voi saada käyttäjän turhautumaan. Tunnistaumisten määrää voidaan laskea yhdistämällä MFA Single sign-on -kirjautumiseen (SSO). SSO on tunnistautumismenetelmä, jonka avulla käyttäjä voi tunnistautua useaan eri järjestelmään yhdellä käyttäjätunnuksella. Tämä tarkoittaa sitä, että käyttäjän ei tarvitse tunnistautua jokaiseen palveluun eri tunnuksilla. (SSO and MFA: The Guide to Overcoming Security Limits n.d.)

Toinen tapa vähentää tarvittavien tunnistautumiskertojen määrää on adaptiivisen MFA:n hyödyntäminen. Adaptiivisessa MFA:ssa käyttäjän täytyy käyttää toista todennustekijää vain silloin, kun tietyt ehdot täyttyvät. Tällaisia tarvittavien todennustekijöiden määrään vaikuttavia tekijöitä voivat olla esimerkiksi epäonnistuneiden kirjautumisyritysten määrä, fyysinen sijainti, käytetyn laitteen tyyppi tai IP-osoite, josta kirjautumisyritys on tehty. (What is Adaptive Multi-Factor Authentication (MFA) n.d.)

7 Pohdinta

7.1 Johtopäätökset

Työn tavoitteena oli selvittää, mitkä ominaisuudet vaikuttavat monivaiheisen tunnistautumisen saavutettavuuteen ja käyttäjäystävällisyyteen, sekä löytää tapoja kehittää tunnistautumisprosessia käyttäjäystävällisemmäksi.

Camp, Das ja Wang selvittivät varmuuskopioinnin, laitteesta toiseen siirtymisen, yhteensopivuuden ja käytön pakollisuuden olevan yleisiä huolenaiheita MFA-sovellusten suhteen. Tämän perusteella käyttäjäystävällisen MFA-sovelluksen pääpiirteitä voisivat olla palvelun mukautuvuus yksilön tarpeisiin, käytön sujuvuus ja käyttäjän motivoiminen vahvemman tunnistautumisen käyttämiseen. Käyttäjäystävällinen tunnistautumisprosessi mukautuu yksilön tarpeisiin tukemalla yhteensopivuutta useiden eri laitteiden kanssa. Tunnistautuminen on sujuvaa, koska tunnistustietojen varmuuskopiointi ja laitteesta toiseen siirtyminen onnistuvat helposti, eikä tunnistautuminen vie

liikaa aikaa. Käyttäjäystävällisen tunnistautumisprosessin taustalla on myös käyttäjän motivoiminen esimerkiksi lisäämällä tietoisuutta monivaiheisen tunnistautumisen tietoturvahyödyistä sekä tietoturvamurron mahdollisista seurauksista.

Saavutettavan tunnistautumisprosessin piirteitä voivat olla esimerkiksi palvelun mukautuminen yksilön tarpeisiin, käytön sujuvuus sekä käytön kuormittavuus. Saavutettava tunnistautumisprosessi mukautuu yksilön tarpeisiin tukemalla yhteensopivuutta erilaisten apuvälineiden kanssa ja tarjoamalla sisältöä eri muodoissa (teksti, kuva tai ääni). Tunnistautuminen on sujuvaa, sillä siihen ei kulu liikaa aikaa ja tunnistautumisprosessi on helppo ja selkeä, jolloin tunnistautuminen epäonnistuu vain harvoin. Toisaalta palvelu myös sietää tahattomia epäonnistuneita tunnistautumisyrityksiä, eikä lukitse käyttäjää ulos palvelusta. Saavutettava tunnistautumisprosessi ei myöskään kuormita käyttäjää vaatimalla liikaa monimutkaisia toimintoja.

7.2 Työn toteutus

Työn tavoitteet saavutettiin ja asetettuihin tutkimuskysymyksiin löydettiin vastaukset. Aiheen tarkempi rajaaminen olisi voinut olla mielekästä. Saavutettavuusvaatimuksia olisi voinut tarkastella esimerkiksi kognitiivisten haasteiden tai näkövamman aiheuttamien erityistarpeiden suhteen, jolloin juuri valitun käyttäjäryhmän kohtaamiin ongelmiin ja niiden ratkaisuihin olisi voinut syventyä tarkemmin.

7.3 Monivaiheisen tunnistautumisen tulevaisuus

Digitalisaation edetessä yhä useammat asiat hoidetaan internetin välityksellä, mikä lisää vahvan tunnistautumisen tarvetta. Digitaalisten palveluiden käyttämistä ei nyky-yhteiskunnassa voi välttää, joten käyttäjäryhmien moninaisuuden huomioiminen on tasa-arvon kannalta välttämätöntä. Saavutettavuuden merkitystä lisää myös väestön ikääntyminen, sillä ikääntyminen tuo mukanaan vaikeuksia näkemisen, fyysisten toimintojen, kuulon ja kognitiivisten toimintojen suhteen (Abou-Zahra, Arch, Miller & Henry 2024).

Lähteet

About Universal Design. N.d. Kuvaus Universal Design -ohjeista. Viitattu 16.04.2024. https://universaldesign.ie/about-universal-design

Abou-Zahra, S., Arch, A., Miller, V. & Henry, S. 2024. Older Users and Web Accessibility: Meeting the Needs of Ageing Web Users. W3C-organisaation ohjeistus ikääntyneiden saavutettavuustarpeista. Viitattu 06.05.2024. https://www.w3.org/WAI/older-users/

Abrams, L. 2022. MFA Fatigue: Hackers' new favorite tactic in high-profile breaches. Artikkeli. Viitattu 30.04.2024. https://www.bleepingcomputer.com/news/security/mfa-fatigue-hackers-new-favorite-tactic-in-high-profile-breaches/

Augoye, V. 2023. How secure is MFA based on SMS and Voice calls. Artikkeli. Viitattu 10.03.2024. https://www.ramsac.com/blog/how-secure-is-mfa-based-on-sms-and-voice-calls/

Authentication Documentation. 2023. Artikkeli. Viitattu 06.03.2024. https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-mfa-number-match

Avouris, M., Belk, M., Fidas, C., Katsini, C. 2016. Security and Usability in Knowledge-based User Authentication: A Review. Konferenssijulkaisu. Viitattu 06.03.2024. https://www.researchgate.net/publication/309195186_Security_and_Usability_in_Knowledge-based_User_Authentication_A_Review

Back up and recover account credentials in the Authenticator app. N.d. Ohje. Viitattu 18.03.2024. https://support.microsoft.com/en-us/account-billing/back-up-and-recover-account-credentials-in-the-authenticator-app-bb939936-7a8d-4e88-bc43-49bc1a700a40

Brezinova, B., Dolezel, M., Drahansky, M. & Urbanek, J. 2012. Influence of Skin Diseases on Fingerprint Recognition. Tutkimusartikkeli. Viitattu 09.04.2024. https://www.researchgate.net/publication/225086704_Influence_of_Skin_Diseases_on_Fingerprint_Recognition

Camp, L., Das, S. Wang, B. 2019. MFA is a Waste of Time! Understanding Negative Connotation Towards MFA Applications via User Generated Content. Viitattu 11.03.2024. https://arxiv.org/ftp/arxiv/papers/1908/1908.05902.pdf

Cisco Accessibility Conformance Report. 2023. Saavutettavuusseloste. Viitattu 13.04.2024. https://www.cisco.com/c/dam/en_us/about/responsibility/accessibility/downloads/vpats/VPAT_Cisco_Duo_Android_v4-12.pdf

Czajka, A., Maciejewicz, P. & Trokielewicz, M. 2019. Iris Recognition in Cases of Eye Pathology. Tutkimusartikkeli. Viitattu 07.04.2024. https://www.researchgate.net/publication/329656959_Iris_Recognition_in_Cases_of_Eye_Pathology

Digipalvelulain vaatimukset. N.d. Aluehallintoviraston ohjeistus digipalvelulaista. Viitattu 07.04.2024. https://www.saavutettavuusvaatimukset.fi/digipalvelulain-vaatimukset/

Furnell, S., Helkala, K., & Woods, N. 2022. Accessible authentication: Assessing the applicability for users with disabilities. Artikkeli. Viitattu 14.04.2024. https://jyx.jyu.fi/handle/123456789/84151

General Data Protection Regulation. 2016. EU:n yleinen tietosuoja-asetuksen johdanto-osan kappale 51. Viitattu 06.03.2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Grother, P., Hanaoka, K., Ngan, M. 2019. Face Recognition Vendor Test (FRVT). Yhdysvaltain standardisointi- ja teknologiainstituutin julkaisema tutkimus. Viitattu 06.03.2024. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

ICF-luokitus. 2024. Terveyden ja hyvinvoinnin laitoksen nettisivuilla julkaistu kuvaus ICF-luokituksesta. Viitattu 14.04.2024. https://thl.fi/aiheet/toimintakyky/icf-luokitus

Involving Users in Evaluating Web Accessibility. 2021. W3C-organisaation ohjeistus käyttäjien osallistumisesta saavutettavuuden arviointiin. Viitattu 27.04.2024. https://www.w3.org/WAI/test-evaluate/involving-users/

Kinzer, K. 2022. What Is Biometric Authentication. Artikkeli. Viitattu 06.03.2024. https://jumpcloud.com/blog/what-is-biometric-authentication

Kuulovammat. N.d. Kuulovammaisuuden määritelmä Kuuloliiton nettisivuilla. Viitattu 07.04.2024. https://www.kuuloliitto.fi/kuulovammat/

Lake, K. 2021. MFA Accessibility: Evaluating Different MFA Factors. Artikkeli. Viitattu 06.03.2024. https://jumpcloud.com/blog/evaluating-the-accessibility-of-different-mfa-factors

Machani, S., M'Raihi, D., Pei, M., Rydell, J. 2011. RFC6238. IETF-organisaation julkaisema standardi. Viitattu 06.03.2024. https://datatracker.ietf.org/doc/html/rfc6238

Microsoft Accessibility Conformance Report. 2023. Saavutettavuusseloste. Viitattu 13.04.2024. https://www.microsoft.com/en-us/accessibility/conformance-reports

Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi. 2023. Opas monivaiheisesta tunnistautumisesta kyberturvallisuuskeskuksen nettisivuilla. Viitattu 06.03.2024. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi

Motoriset taidot – mitä ne ovat? N.d. Artikkeli. Viitattu 12.04.2024. https://innostunliikkumaan.fi/motoriset-taidot-arjessa-ja-niiden-oppimiseen-vaikuttavat-tekijat/motoristen-taitojen-oppimiseen-vaikuttavat-tekijat/

Multifactor Authentication Cheat Sheet. N.d. Kuvaus monivaiheisesta tunnistautumisesta Open Worldwide Application Security Projectin nettisivuilla. Viitattu 06.03.2024. https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html

Näkövammaisuus. 2022. Näkövammaisten liiton määritelmä näkövammaisuudesta. Viitattu 07.04.2024. https://www.nakovammaistenliitto.fi/fi/nakovammaisuus#header--nakovammaisuuden-maaritys

TEPA-termipankki. 2002. Viitattu 06.03.2024. https://termipankki.fi/tepa/fi/haku/käyttäjäystävällisyys

Vilkka, H. 2023. Kirjallisuuskatsaus metodina, opinnäytetyön osana ja tekstilajina. E-kirja. Viitattu 08.04.2024.

Vuoksimaa, M. 2019. Kognitiivisten toimintojen muutokset – mikä on ikääntymistä, mikä sairautta? Artikkeli. Viitattu 07.04.2024. https://www.duodecimlehti.fi/duo14952

Web Content Accessibility Guidelines. 2023. WC3-organisaation ohjeistus verkkosisällön saavutettavuudesta. Viitattu 16.04.2024. https://www.w3.org/TR/WCAG21/

What is Adaptive Multi-Factor Authentication (MFA)? N.d. Artikkeli. Viitattu 20.04.2024. https://www.cyberark.com/what-is/adaptive-mfa/

What is shadow IT. N.d. Artikkeli. Viitattu 04.04.2024. https://www.cloudflare.com/learning/access-management/what-is-shadow-it/

What is a push notification. N.d. Artikkeli sivustolla ibm.com. Viitattu 06.03.2024. https://www.ibm.com/topics/push-notifications

What Is a Security Token. 2023. Artikkeli. Viitattu 06.03.2024. https://www.okta.com/identity-101/security-token/

What is Usability Evaluation? 2016. Artikkeli. Viitattu 27.04.2024. https://www.interaction-design.org/literature/topics/usability-evaluation

Molinaro, D. 2023. What Is a SIM Swap Attack and How Can You Prevent It? Artikkeli. Viitattu 19.04.2024. https://www.avast.com/c-sim-swap-scam

Selecting Web Accessibility Evaluation Tools. 2023. W3C-organisaation ohjeistus saavutettavuustestaustyökalun valinnasta. Viitattu 27.04.2024. https://www.w3.org/WAI/test-evaluate/tools/selecting/

Soegaard, M. 2023. System Usability Scale for Data-Driven UX. Artikkeli. Viitattu 27.04.2024. https://www.interaction-design.org/literature/article/system-usability-scale

SSO and MFA: The Guide to Overcoming Security Limits. N.d. Artikkeli. Viitattu 20.04.2024. https://www.trustbuilder.com/sso-mfa

Yleistä saavutettavuudesta. N.d. Yleinen kuvaus saavutettavuudesta Aluehallintoviraston saavutettavuudesta kertovilla nettisivuilla. Viitattu 06.03.2024. https://www.saavutettavuusvaatimukset.fi/yleista-saavutettavuudesta/