Mobiililaitteiden biometriset tunnistusmenetelmät: Ratkaisut, käyttökokemukset ja haasteet yksityiskäyttäjän näkökulmasta

Olmo Kosunen

Haaga-Helia ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Amk-opinnäytetyö
2024

Tiivistelmä

Tekijä(t)
Olmo Kosunen

Tutkinto
Tradenomi

Opinnäytetyön nimi
Mobiililaitteiden biometriset tunnistusmenetelmät: Ratkaisut, käyttökokemukset ja haasteet yksityiskäyttäjän näkökulmasta

Sivu- ja liitesivumäärä
49 + 12

Käyttäjän tunnistamisen rooli mobiililaitteilla on tärkeässä osassa, sillä se suojaa käyttäjän henkilökohtaisia tietoja estämällä luvattoman pääsyn mobiililaitteisiin. Mobiililaitteiden biometriset tunnistusmenetelmät tarjoavat käyttäjille turvallisen sekä vaivattoman tavan varmentaa pääsyn laitteelle ilman perinteisiä tunnuslukuja tai salasanoja.

Tässä opinnäytetyössä tutkitaan aluksi tietoperustan kautta, miten mobiililaitteiden biometriset tunnistusmenetelmät kuten sormenjälki-, kasvojen- sekä iiristunnistin ja niiden erilaiset versiot toimivat perusperiaatteiltaan. Lisäksi tietoperustassa avataan niiden toimintaperiaatetta yleisimmissä mobiililaitteiden käyttöjärjestelmissä ja käydään läpi yleisimmin ilmenneitä haasteita. Tietopohjassa käydään myös läpi aikaisempia tutkimuksia aiheesta, joiden tuloksia verrataan tästä opinnäytetyöstä saatuihin uusiin tuloksiin. Opinnäytetyössä tutkitaan kyselyn avulla, miten yksityiskäyttäjät kokevat mobiililaitteiden biometriset tunnistusmenetelmät niiden käytettävyyden ja tietotuvallisuuden osalta, mitä haasteita niiden käytössä ilmenee sekä mitkä biometriset tunnistusmenetelmät olivat opinnäyteyön tekemishetkellä suosiossa.

Opinnäytetyön tutkimustulokset perustuvat määrällisenä tutkimusmenetelmänä käytettyyn verkkokyselyyn, sekä tietoperustasta saatuihin pohjatietoihin. Kyselytutkimukseen vastasi 56 vastaajaa ja kysely suoritettiin aikavälillä 8.3.-24.3.2024.

Tutkimustulosten perusteella biometristen tunnistusmenetelmien käytettävyys koettiin olevan hyvällä tasolla. 75 % vastaajista on ollut useimmiten tyytyväisiä käyttämäänsä biometriseen tunnistusmenetelmään. Sormenjälkitunnistin koettiin käytettävyyden osalta hieman paremmaksi kuin kasvojentunnistin. Tuloksista voidaan todeta, että biometristen tunnistusmenetelmien nykyinen taso on saavuttanut hyvän käytettävyyden. Iiristunnistin ei ollut suosittu vaihtoehto, ja sen käyttö on ollut vähäistä tutkimuksen perusteella, sillä vain 2 vastaajaa on käyttänyt sitä.

Biometrisiä tunnistusmenetelmiä pidettiin yleisesti luotettavina. Vastaajat kokivat sormenjälkitunnistimen olevan tietoturvallisin vaihtoehto, kun taas kasvojentunnistin koettiin hieman turvattomampana. Tutkimustuloksista voidaan todeta, että yksityiskuluttajat suosivat biometrisistä tunnistusmenetelmistä eniten sormenjälkitunnistinta, mutta kasvojentunnistin on nostanut suosiotaan viime vuosien aikana johtuen Applen päätöksestä luopua sormenjälkitunnistuksesta.

Biometristen tunnistusmenetelmien kanssa ilmeni paljon haasteita tunnistamisen yhteydessä, joita voidaan korjata ottamalla opinnäytetyössä esiteltyjä uusia teknologioita käyttöön. Opinnäytetyön tulosten perusteella biometristen tunnistusmenetelmien kehityksessä voidaan kiinnittää huomiota käytettävyyden parantamiseen ja uusien teknologioiden hyödyntämiseen.

Asiasanat
Biometrinen tunnistusmenetelmä, mobiililaite, käytettävyys, tietoturva, kysely, kokemus

Sisällys

1 Johdanto

Tämän opinnäytetyön aiheeksi valikoitui mobiililaitteiden biometriset tunnistusmenetelmät. Yleisesti kuluttajien saatavilla olevat biometriset tunnistusmenetelmät mobiililaitteissa ovat suhteellisen uutta teknologiaa ja ne kehittyvät koko ajan. Lisäksi olen töissäni Helsingin keskustakirjasto Oodissa ja Haaga-Helian IT-tuessa auttanut asiakkaita paljon niiden kanssa. Tämän takia koen biometristen tunnistusmenetelmien olevan ajankohtainen ja mielenkiintoinen aihe. Olen huomannut niiden aiheuttavan paljon hankaluuksia ja epäluuloa etenkin vanhempien ihmisten keskuudessa. Henkilökohtaisesti olen käyttänyt biometrisistä tunnistusmenetelmistä sormenjälki- ja kasvojentunnistinta monissa älypuhelimissa ja kannettavissa tietokoneissa jo vuodesta 2016 lähtien ja kokenut myös ongelmia matkalla. Ongelmina on ollut muun muassa tunnistustapahtuman epäonnistumista monista syistä.

Viime vuosina siirtyminen perinteisistä salasanoista ja PIN-koodeista biometrisiin tunnistusmenetelmiin on helpottanut mobiililaitteiden näytönlukituksen ja suojattujen sovellusten avaamista ja näin nopeampaa pääsyä sovelluksiin kuten verkkopankkiin ja muihin henkilökohtaisiin tietoihin. Samalla herää kuitenkin huoli laitteilla olevien henkilökohtaisten tietojen tietoturvasta.

Mahdollinen hyökkääjä voi saada pääsyn moniin henkilökohtaisiin tietoihin vain avaamalla mobiililaitteen näytönlukituksen. Lisäksi käyttäjän mobiilipalvelut ja sovellukset ovat alttiita erilaisille turvallisuusuhille, kuten luvattomille toimille, esimerkiksi verkko-ostoksille ja haittaohjelmien asennuksille, hyödyntämällä käyttäjän mobiililaitetta. (Wang, Wang, Chen, Liu, Liu 2020, 1.)

Käyttäjän tunnistamisen rooli mobiililaitteilla on elintärkeää, sillä se suojaa käyttäjän herkkiä henkilökohtaisia tietoja ja estää luvattoman pääsyn mobiililaitteisiin. Tässä yhteydessä biometrinen tunnistaminen nousee esiin tehokkaana ratkaisuna, joka perustuu yksilöllisiin biologisiin liittyviin piirteisiin. Biometrinen tunnistaminen tarjoaa käyttäjille turvallisen ja vaivattoman tavan varmentaa henkilöllisyytensä ilman perinteisiä tunnuslukuja tai salasanoja ja niiden muistamisen aiheuttamaa vaivaa. (Wang, Wang ym. 2020, 1.)

1.1 Opinnäytetyön rajaus

Tässä opinnäytetyössä keskitytään mobiililaitteiden biometristen tunnistusmenetelmien haasteisiin niiden tekniseltä taustalta. Biometristen tunnistusmenetelmien kanssa on paljon haasteita myös muun muassa lainsäädännön näkökulmasta, mutta tämä aspekti rajattiin pois siitä syystä, että muuten opinnäytetyöstä olisi tullut liian laaja.

1.2 Opinnäytetyön tavoite

Opinnäytetyön tavoitteena ja pääkysymyksenä on selvittää, miten yksityiskäyttäjät eli tavalliset kuluttajat kokevat mobiililaitteiden erilaiset biometriset tunnistusmenetelmät käytettävyyden ja tietoturvallisuuden osalta. Yksityiskäyttäjille opinnäytetyöni lisää tietoisuutta ja tietämystä biometrisistä tunnistusmenetelmistä ja auttaa heitä ymmärtämään eri vaihtoehtoja ja niiden toimintaperiaatteita. Analysoimalla ratkaisuja ja haasteita voin jakaa tietoa, jotka parantavat biometristen tunnistusmenetelmien turvallisuutta ja käyttäjäystävällisyyttä, mikä voi täten vaikuttaa suoraan yksityiskäyttäjien mobiililaitteiden käyttökokemukseen. Tietoperustan tavoitteena on toimia pohjana kyselylle sekä selittää teknologiaa biometristen tunnistusmenetelmien taustalla. Itse kyselyn tavoitteena on saada hyödyllistä käyttäjätietoa siitä, mitä biometrisiä menetelmiä käytetään, miten ne koetaan ja mitä haasteita kuluttajat ovat kohdanneet.

Mobiililaitteiden valmistajille tutkimus voi antaa uuttaa päivitettyä tietoa siitä, miten käyttäjät kokevat ja arvioivat eri biometrisiä tunnistusmenetelmiä. Tämä voi ohjata uusien tunnistusmenetelmien suunnittelua ja tuotekehitystä. Tutkimus antaa siis valmistajille mahdollisuuden arvioida ja parantaa biometristen tunnistusmenetelmien käyttäjäkokemusta ja turvallisuutta omilla laitteillaan.

Tutkimus voi myös antaa pohjan jatkotutkimukselle liittyen biometristen tunnistusmenetelmien kehitykseen ja parannuksiin.

Pääkysymykseen haetaan lisäksi vastauksia alla olevien alaongelmien kautta:

1. Suosivatko yksityiskäyttäjät sormenjälki-, kasvojen- vai iiristunnistinta biometrisistä tunnistusmenetelmistä?
2. Mitä haasteita yksityiskäyttäjät ovat kohdanneet biometrisiin tunnistusmenetelmiin liittyen?

1.3 Keskeiset käsitteet

Android Googlen kehittämä mobiililaitteiden käyttöjärjestelmä (Erica Mixon 2023).

Biometrinen tunnistus-menetelmä	Henkilöllisyyden todentamista yksilöllisellä fyysisellä ominaisuudella, kuten kasvot, sormenjälki tai silmän iiris (Ajankohtaista 2023).
Face ID	Applen kehittämä kasvojentunnistusteknologia (Apple 28.8.2023).
Iiris-skannaus	Biometrinen tunnistusmenetelmä, joka käyttää silmän iiriksen yksilöllisiä piirteitä henkilön tunnistamiseen (TechTerms 2023a).
iOS	Applen mobiililaitteille kehittämä käyttöjärjestelmä, joka on suunniteltu toimimaan yhtiön mobiililaitteissa, kuten iPhoneissa ja iPadeissä (Sweeney 7.7.2024).
Kasvojentunnistin	Biometrinen tunnistusmenetelmä, joka perustuu kasvojen ainutlaatuisiin piirteisiin, kuten kasvojen muotoon, silmiin ja nenään. Se käyttää kamerajärjestelmiä ja erityisiä algoritmeja tunnistamaan yksilöitä. Kasvojentunnistusta käytetään laajasti älypuhelimissa ja tietokoneissa. (TechTerms 2023b.)
Lippulaiva	Tuotemalliston paras tuote (Britannica 2024).
Mobiililaite	Laite, joka on suunniteltu mukana kannettavaksi. Näitä laitteita ovat esimerkiksi älypuhelimet, tabletit ja kannettavat tietokoneet. (Tietotekniikan termitalkoot 2005.)
PIN-koodi	Henkilökohtainen numerokoodi, joka käytetään yleensä tunnistautumiseen ja tietoturvaan älypuhelimissa, tietokoneissa ja muissa laitteissa (TechTerms 2023c).
Salasana	Salainen merkkijono, jota käytetään tunnistautumiseen ja pääsyn suojaamiseen esimerkiksi älypuhelimissa ja tietokoneissa. Se on henkilökohtainen ja tarkoitettu vain käyttäjän tiedossa olevaksi. (TechTerms 2023d.)

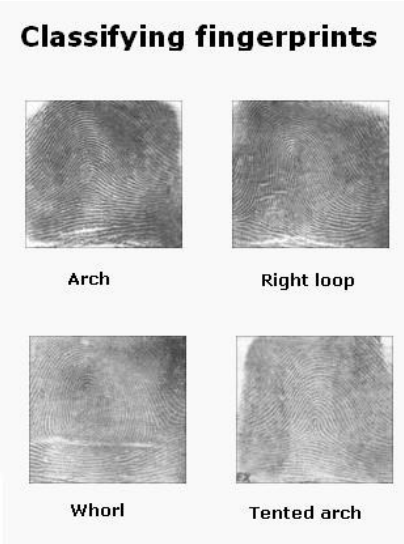
Sormenjälkitunnistin	Biometrinen tunnistusmenetelmä, joka perustuu yksilön sormenjäljen ainutlaatuisuuteen. Se käyttää sormenjäljen analysointia ja tallentamista tunnistustarkoituksiin, kuten pääsynvalvontaan tai laitteen avaamiseen. Sormenjälkitunnistusta käytetään yleisesti älypuhelimissa ja tietokoneissa. (TechTerms 2023e.)
Touch ID	Applen kehittämä sormenjälkitunnistusteknologia, joka on ensisijaisesti käytössä iPhone- ja iPad laitteissa (Apple 15.11.2023).
Windows 10	Microsoftin kehittämä käyttöjärjestelmä, joka on suunniteltu tietokoneille, tableteille ja hybridilaitteille. Se on osa Windows-käyttöjärjestelmien perhettä ja se julkaistiin ensimmäisen kerran heinäkuussa 2015. (Bigelow 2022.)
Windows Hello	Microsoftin kehittämä biometrinen tunnistusjärjestelmä, joka mahdollistaa käyttäjien kirjautumisen Windows 10 -käyttöjärjestelmään turvallisesti ilman salasanaa. Windows Hello tukee useita biometrisiä tunnistusmenetelmiä, kuten sormenjälkitunnistusta, kasvojentunnistusta ja iirisskannausta. (Microsoft 11.5.2023.)

2 Biometrinen tunnistaminen

Mobiililaitteissa biometrisiä tunnistusmenetelmiä on otettu laajalti käyttöön lisäämään tietoturvallisuutta ja käyttäjämukavuutta. Biometrinen tunnistaminen tarkoittaa yksilöllisiin fyysisiin ominaisuuksiin perustuvia henkilöllisyyden tunnistusmenetelmiä. Näitä ominaisuuksia voivat olla esimerkiksi sormenjälki, kasvonpiirteet ja silmän iiris. Biometristen tunnistusmenetelmien tarkoituksena on tarjota turvallinen ja tehokas tapa varmentaa henkilöllisyys, sillä jokainen yksilöllinen biometristen ominaisuuksiensa osalta. (Jain, Ross & Prabhakar 2004, 1.) Seuraavissa luvuissa käydään läpi biometrisistä tunnistusmenetelmistä sormenjälkitunnistin, kasvojentunnistin ja iiristunnistin, sekä niiden eri toteutustapoja.

2.1 Sormenjälkitunnistin

Sormenjälkitunnistaminen on yksi vanhimmista tavoista tunnistaa yksilö, joka perustuu jokaisella henkilöllä olevaan ainutlaatuiseen sormenjälkeen. Sormenjälki on jälki sormen tai sormen osan uurteista (kuva 1). Uurteet ovat koholla oleva osa sormien ihoa, koostuen yhdestä tai useammasta yhteen liitetystä ihon harjun ”uureyksiköstä”. (Kodituwakku 2015, 115.)



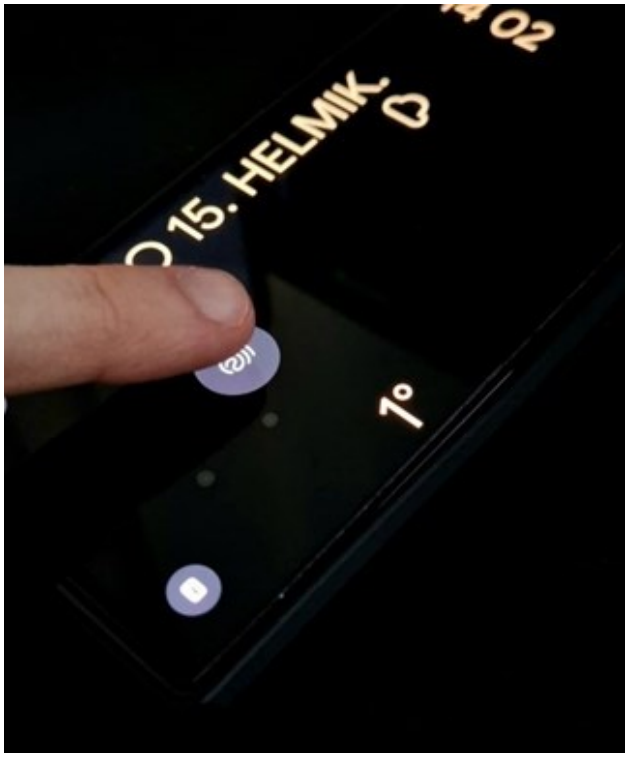
Kuva 1. Sormenjäljen uurteiden eri tyyppejä (Ivanova 2006 CC BY 2.0)

Sormenjäljen lukemiseen ja tunnistamiseen on monia eri tekniikoita ja mobiililaitteiden sormenjälkitunnistimissa yleisin käytetty teknologia on optinen sensori, joko näytön alla tai erillisenä lukijana laitteessa, joka lukee sormen uurteet. Kapasitiiviset sormenjälkitunnistimet ovat myös suosittuja. (Triggs 25.3.2023.) Myös ultra-ääneen perustuvia sormenjälkitunnistimia on käytössä (Kodituwakku 2015, 115).

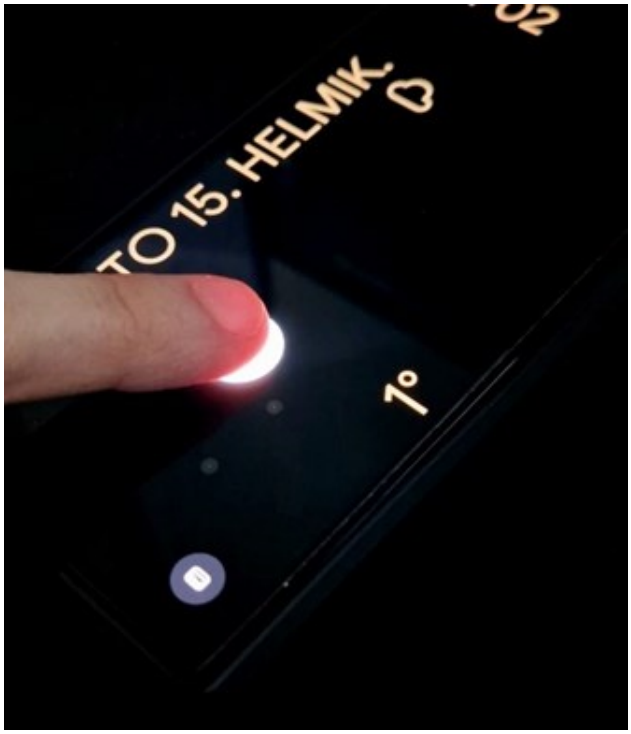
Jos käy elektroniikkaliikkeissä katsomassa uusia mobiililaitteita, niin melkein kaikissa uusissa Android -puhelimissa ja tableteissa ja hieman vanhemmissa Applen laitteissa, sekä monissa kannettavissa tietokoneissa on käytössä sormenjälkitunnistin. Seuraavissa luvuissa käydään läpi eri tapoja toteuttaa sormenjälkitunnistimia mobiililaitteissa.

2.1.1 Optinen sormenjälkitunnistin

Optisen sormenjälkitunnistimen toiminta perustuu sormenjälkilukijassa olevan kameran ottamaan kuvaan. Sen jälkeen algoritmi havaitsee kuvasta ainutlaatuiset kuviot sormen pinnasta analysoimalla kuvan vaaleimpia ja tummimpia alueita. Optisten sormenjälkitunnistimien kameroissa on rajallinen resoluutio, joten mitä tarkempi sensori lukijassa on, sitä turvallisempi se on. Optiset sormenjälkitunnistimet sijaitsevat mobiililaitteiden näyttöjen alla (kuva 2), joten optisen sormenjälkitunnistimen kameran sensori tarvitsee valoa. Tätä varten näytön paneelin pikselit aktivoituvat lukijan kohdalla toimien salamana (kuva 3) tai sensoriin on rakennettu omaa valoa tuottava elementti. (Triggs 25.3.2023.)



Kuva 2. Optinen sormenjälkitunnistin näytön alla



Kuva 3. Optisen sormenjälkilukijan "salama" lukutilanteessa

Optisten sormenjälkitunnistimien suurin tietoturvaan liittyvä heikkous on se, että niiden huijaaminen on melko helppoa. Koska optisten sormenjälkitunnistimien tekniikka perustuu sormesta otettuun kaksiulotteiseen kuvaan, sormenpään proteeseja ja hyvälaatuisia kuvia voidaan käyttää optisen sormenjälkitunnistimen murtamiseen. (Triggs 25.3.2023.)

2.1.2 Kapasitiivinen sormenjälkitunnistin

Kapasitiivinen sormenjälkitunnistus on yksi yleisesti käytetty menetelmä, ja se esiintyy yleensä älypuhelimien etu-, sivu- ja takaosissa (kuvat 4, 5). Kapasitiiviset somenjälkitunnistimet ovat maineeltaan turvallisia, ja niiden toiminta perustuu kondensaattoriin. (Triggs 25.3.2023.)

Kuva 4. Kapasitiivinen sormenjälkitunnistin älypuhelimen takaosassa

Kuva 5. Kapasitiivinen sormenjälkitunnistin älypuhelimen sivuosassa

Toisin kuin edellisessä luvussa esitelty optinen sormenjälkitunnistin, kapasitiiviset sormenjälkitunnistimet käyttävät siis pieniä kondensaattoripiirejä sormenjälkitietojen keräämiseen. Kondensaattorit varastoivat sähkövarausta, ja kun ne yhdistetään johtaviin levyihin sormenjälkitunnistimen pinnalla, ne mahdollistavat sormenjäljen tunnistamista vaativien yksityiskohtien seuraamisen. Sormenpään asettaminen johtavien levyjen päälle muuttaa varastoitua varausta hieman, kun taas ilmarako sormen ja sormenjälkitunnistimen välillä säilyttää varaustason suhteellisen ennallaan. Varauksen muutokset seurataan käyttämällä operaatiovahvistinta ja tallennetaan sitten analogia-digitaalimuuntimella. Digitaalinen data analysoidaan sen jälkeen erottuvien ja ainutlaatuisten sormenjälkimääritteiden tunnistamiseksi, ja ne tallennetaan myöhempää vertailua varten. (Triggs 25.3.2023.)

Suuren kondensaattorijoukon kokoaminen sormenjälkitunnistimeen mahdollistaa erittäin yksityiskohtaisen sormenjäljen kuvan luomisen pelkästään sähkösignaaleista. Kuten optisessa sormenjälkitunnistimen kameran resoluution kanssa, enemmän kondensaattoreita tuottaa korkeamman resoluution tunnisteen. Tämä lisää optisen sormenjälkilukijan turvallisuustasoa, mutta suuren kondensaattorijoukon tiheyden tuottaminen tuo mukanaan suuremmat tuotantokustannukset. (Triggs 25.3.2023.)

Kapasitiivista sormenjälkitunnistinta on vaikeampi huijata kuin optista sormenjälkitunnistinta, koska sitä ei voi huijata pelkällä kuvalla sormenjäljestä. Lisäksi sitä on erittäin vaikea huijata sormenpään proteeseilla, sillä eri materiaalit aiheuttavat hieman erilaisia varauksen muutoksia kondensaattorissa. Kapasitiivisten sormenjälkitunnistimien turvallisuusriskit liittyvät itse laitteiston tai ohjelmiston hakkerointiin. (Triggs 25.3.2023.)

2.1.3 Optiskapasitiivinen sormenjälkitunnistin

Tietoturvahaasteet ovat saaneet älypuhelimien valmistajat siirtymään optiskapasitiivisiin hybridisormenjälkilukijoihin. Optiskapasitiiviset sormenjälkilukijat yhdistävät optisen sormenjälkiteknologian kapasitiiviseen tunnistukseen, mikä mahdollistaa tarkemman sormenjäljen havaitsemisen. (Triggs 25.3.2023.)

Optiskapasitiiviset sormenjälkitunnistimet korjaavat aiempien optisten mallien tietoturvaongelmia yhdistämällä kapasitiivisten sormenjälkitunnistimien vaativan "oikean kosketuksen" optisten sormenjälkitunnistimien nopeuteen ja energiatehokkuuteen. Optiskapasitiiviset sormenjälkitunnistimet sijaitsevat laitteiden näyttöjen alla. (Triggs 25.3.2023.)

2.1.4 Ultraääneen perustuva sormenjälkitunnistin

Ultraääneen perustuvat sormenjälkilukijat ovat uusinta uutta älypuhelimissa, mutta nykyään kalleimmissa uusissa Android -älypuhelimissa alkaa olemaan niitä. Ultraääneen perustuvat sormenjälkitunnistimet ovat sormenjälkilukijoista turvallisin vaihtoehto niiden kolmiulotteisen luonteen takia. (Triggs 25.3.2023.)

Yhdysvaltalainen puolijohdevalmistaja Qualcomm on ollut tärkeässä roolissa niiden kehittämisessä. Qualcommin 3D ultraäänisormenjälkitunnistin on sittemmin otettu käyttöön Samsungin lippulaivoissa, mukaan lukien uusimmat Galaxy S22 ja Galaxy S23. Samsung väittää, että uusi skanneri on 77 % suurempi ja 50 % nopeampi kuin edellisen sukupolven tuote. (Thomas 1.10.2021.)

Sormenjälkien tallentamiseksi ultraäänen perustuvissa sormenjälkitunnistimissa käytetään, sekä lähettävää, että vastaanottavaa ultrasoniikkakomponenttia. Kun sormi asetetaan tunnistimen päälle, lähetetään ultraäänipulssi, joka osittain imeytyy sormeen ja osittain heijastuu takaisin anturiin. Heijastuneiden signaalien intensiteetti mitataan mekaanisen rasituksen havaitsevan anturin avulla eri kohdissa sormenjälkitunnistinta. (Triggs 25.3.2023.)

Ultraääneen perustuvan sormenjälkitunnistimen 3D-luonne tekee siitä turvallisemman vaihtoehdon kapasitiivisille ja optisille sormenjälkitunnistimille. Ultraäänitekniikka on kuitenkin aiheuttanut haasteita tietyntyyppisten näytönsuojien kanssa, erityisesti paksumpien suojien kanssa, mikä voi vaikuttaa menetelmän tarkkuuteen. (Triggs 25.3.2023.) Samsung joutuikin julkaisemaan korjaustiedostoja älypuhelimiinsa korjatakseen ongelmat, jotka mahdollistivat melkein minkä tahansa sormenjäljen käyttämisen puhelimen lukituksen avaamiseen puhelimen käytettäessä näytönsuojaa (Dent 17.10.2019). Ultraääntä käyttävät sormenjälkilukijat ovat myös toimivuuden osalta parempia verrattuna aikaisemmin esiteltyihin lukijoihin, koska ne toimivat jopa veden alla ja märillä käsillä (Brant 28.6.2017).

2.1.5 Sormenjälkitunnistin Android -laitteilla

Maailman kahdessa suosituimmassa mobiililaitteiden käyttöjärjestelmissä Androidissa ja Applen iOS käyttöjärjestelmässä (Statcounter 2023), on molemmissa sormenjälkitunnistusteknologiaa ja hieman erilaiset ratkaisut. Seuraavissa luvuissa tarkastellaan niiden toimintamalleja.

Googlen kehittämässä Android -käyttöjärjestelmässä sormenjälkitunnistimen toiminta perustuu käyttöjärjestelmässä olevaan BiometricPrompt -ohjelmointirajapintaan, joka tukee sormenjälkitunnistamista. Android tallennuttaa sormenjälkitietoja ainoastaan puhelimen omaan salattuun muistiin, eikä tietoja jaeta Googlelle tai puhelimen muille sovelluksille. (Android Open Source Project 2024a.)

Android käyttöjärjestelmällä olevia laitteita tulee monelta eri valmistajalta, joten sormenjälkilukijan tyypin mukaan on olemassa monia erilaisia ratkaisuja. Jotta laitetoteutusten katsotaan olevan yhteensopivia Androidin kanssa, niiden on täytettävä Android Compatibility Definition Document (CDD) -asiakirjassa esitetyt vaatimukset (Android Open Source Project 2024b). Kaikkien uusien Android -laitteiden sormenjälkitunnistin käyttää Fingerprint Hardware Interface Definition Language (HIDL) -kieltä muodostaakseen yhteyden valmistajakohtaiseen kirjastoon ja sormenjälkilaitteistoon (Android Open Source Project 2024c).

Google varoittaa oman tuotteensa Pixel -puhelimien sivuilla, että sormenjälkitunnistin voi olla vähemmän turvallinen tapa suojata puhelin, kuin vahva PIN-koodi tai salasana. Google varoittaa, että kopiota sormenjäljestä voi käyttää laitteen avaamiseen. (Google s.a. a.)

2.1.6 Sormenjälkitunnistin Apple -laitteilla

Apple alkoi asteittain siirtymään pois älypuhelimien sormenjälkitunnistamisesta vuonna 2017, koska yhtiö piti kasvojentunnistusta turvallisempana kuin sormenjälkitunnistinta (Feldman 12.7.2017). Applen sormenjälkilukijat poistuivat sen älypuhelimista iPhone SE (2022) mallin jälkeen, mutta yhtiön iPad ja MacBook laitteissa sorrmenjälkitunnistimet ovat vielä käytössä uusissa laitteissa (Edwards 2022).

Tekniseltä toteutukseltaan Applen Touch ID -sormenjälkitunnistin käyttää kapasitiivista lukijaa tallentaakseen korkearesoluutioisen kuvan sormenjäljen pienistä osista. Se luokittelee sormenjäljen tyypin ja kartoittaa yksityiskohtia, jotka ovat huokosten ja reunarakenteiden aiheuttamia. Applen mukaan turvallisuusominaisuudet sisältävät 1: 50 000 todennäköisyyden virheellisestä tunnistuksesta ja vain viisi epäonnistunutta yritystä ennen salasanan vaatimista. Applen sirun oma Secure Enclave -arkkitehtuuri suojaa sormenjälkitietoja, eikä tietoja tallenneta muualle. (Apple 15.11.2023.)

2.1.7 Uutta tutkimustietoa sormenjäljen ainutlaatuisuudesta ja sen soveltamisesta mobiililaitteissa

Uudessa vuonna 2024 julkaistussa Columbian yliopiston tutkimuksessa on havaittu, vastoin yleistä olettamusta, että saman henkilön kaksi eri sormista otettua sormenjälkeä ovat hyvin samankaltaisia. Tästä uudesta tutkimustuloksesta voi olla hyötyä sormenjälkitunnistimien kehityksessä. Tutkijoiden kehittämän sormenjälkien käsittelylaitteiston avulla henkilö voi rekisteröityä laitteensa sormenjälkitunnistimeen yhdellä sormella ja avata sen lukituksen millä tahansa toisella sormella. Tämä voi lisää sormenjälkitunnistimen käytettävyyttä, ja se on hyödyllistä myös tilanteissa, joissa käyttäjän sormenjälkitunnistukseen rekisteröity sormi on tilapäisesti tai pysyvästi lukukelvoton, vaikka laastarin, lian tai sormeen kohdistuneen onnettomuuden vuoksi. (Guo ym. 2024, 1, 6.)

Toki Applen iOS sekä Googlen Android käyttöjärjestelmät ovat mahdollistaneet käyttäjille viiden eri sormenjäljen lisäämisen laitteelle, joten käyttäjillä on ollut jo mahdollisuus avata mobiililaitteensa lukitus monella eri sormella (Apple 15.11.2023; Google s.a. a). Monen sormenjäljen lisääminen on kuitenkin aikaa vievä prosessi.

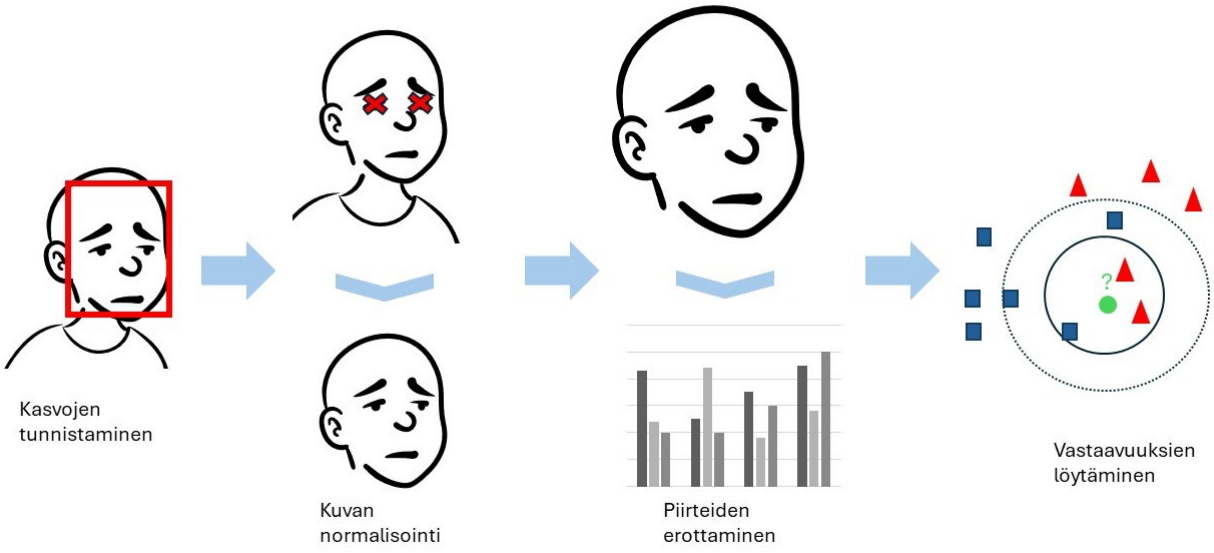
2.2 Kasvojentunnistin

Kasvojentunnistustekniikka tunnistaa tai varmentaa henkilön automaattisesti digitaalisesta kuvasta tai videon ruutukehyksestä käyttäen mobiililaitteen etukameraa. Kasvojentunnistus perustuu

tiettyihin kasvonpiirteisiin, kuten silmien, nenän ja suun sijaintiin, sekä näiden piirteiden välimatkoihin. Näistä ominaisuuksista kerätyt tiedot tallennetaan kuvatietokantaan. (Kodituwakku 2015c, 117.) Käyttäjän avatessa mobiililaitettaan, etukamera aktivoituu ja vertaa kasvoja tietokannassa olevaan tietoon (Moorthy, Raaj, Akshayaa & Manoj 2023, 2072). Kasvojentunnistuksessa on käytössä erilaisia teknologioita, joita käydään läpi seuraavissa kappaleissa.

2.2.1 Etukameraan perustuva kasvojentunnistin

Etukameraan perustuvassa menetelmässä otetaan tavallinen kaksiulotteinen kuva kasvoista ja kasvojen alue normalisoidaan (kuva 6) kiinteään ennalta määriteltyyn kokoon, ja normalisoitua kaksiulotteista kuvaa kutsutaan kanoniseksi kuvaksi. Tämän jälkeen lasketaan kasvojenmittauksesta saadut tiedot, jotka tallennetaan vastaavaan kasvomalliin. (Kodituwakku 2015d, 117.)



Kuva 6. Kasvojentunnistuksen tapahtumaketju (mukaillen Jain, Klare & Park 2012)

Kun laitetta ryhtyy avaamaan laitteiston algoritmit vertaavat etukameran näkemää kuvaa, sen tietokannassa olevaan referenssikuvaan. Tämän menetelmän heikkous on vaihtelevat valaistusolosuhteet ja yksinkertaisuus. (Wankhede 16.8 2022.)

2.2.2 Infrapunaan perustuva kasvojentunnistin

Infrapunaan perustuva kasvojentunnistus tarjoaa turvallisemman vaihtoehdon verrattuna perinteiseen pelkkään kamerapohjaiseen kasvojentunnistukseen, joka käyttää valon näkyvää spektriä. Tämä menetelmä edellyttää lisälaitteistoa, kuten infrapunavaloa ja kameraa, joka kykenee havaitsemaan infrapunaspektrin. Infrapunaan perustuva kasvojentunnistus toimii samalla periaatteella kuin viime luvun etukameraan perustuva kasvojentunnistus, mutta se tapahtuu infrapunaspektrissä. Tämä tekee menetelmän huijaamisesta huomattavasti vaikeampaa pelkällä valokuvalla. Infrapunan käyttö varmistaa myös tasaisen toimivuuden eri valaistusolosuhteissa. Vaikka infrapunaan perustuva kasvojentunnistus ei ole vielä kovin yleinen, se tarjoaa edullisemman vaihtoehdon verrattuna huippuluokan 3D-kuvaan perustuviin kasvojentunnistimiin. (Triggs 14.1 2019.)

2.2.3 3D-kuvaan perustuva kasvojentunnistin

3D-kuvaan perustuvassa kasvojentunnistamisessa kolmiulotteisen kuvan saamiseksi tunnistukseen käytetään liikkuvaa kuvaa, eli käytännössä kasvot käännetään puolelta toiselle (kuva 9), jotta saadaan muodostettua puolipyöreä kuva, jonka keskellä on tunnistettavan henkilön kasvot. Tämän jälkeen voidaan generoida tunnistuksen vaativa kolmiulotteinen kuva. Kulmakarvojen, silmien, nenän, suun, leuan ja otsan sijainti ja etäisyys silmien ja kulmakarvojen välillä lasketaan ja tallennetaan kasvomalliin. Tämän menetelmän luotettavuus on korkea verrattuna kaksiulotteisiin kuviin perustuvaan menetelmään. (Kodituwakku 2015e, 117.) Toinen ratkaisu 3D -kasvojentunnistamiseen on käyttää lisäksi infrapunaa ja muita sensoreita muodostamaan 3D- kuvan kasvoista (Apple 22.8.2023). Tällä hetkellä 3D-kasvojentunnistus on ainoa markkinoilla oleva kasvojentunnistusmenetelmä, joka on riittävän turvallinen käytettäväksi mobiilimaksamiseen (Triggs 14.1 2019).

Kuva 7. Puolipyöreän kuvan saaminen kolmiulotteista kasvojentunnistusta varten (mukaillen Apple s.a)

2.2.4 Kasvojentunnistus Android -laitteilla

Android -laitteissa kasvojentunnistaminen perustuu jälleen BiometricPrompt ohjelmointirajapintaan, joka tukee kasvojentunnistamista (Android Open Source Project 2024b). Face Authentication Hardware Interface Definition Language (HIDL) -kieli muodostaa yhteyden laite ja valmistajakohtaisiin kirjastoihin (Android Open Source Project 2024e). Verrattuna Android -laitteissa oleviin sormenjälkilukijoihin, kasvojentunnistamisessa on enemmän variaatiota sen luotettavuudessa riippuen laitteen valmistajan ratkaisusta (Hristov 16.8.2022).

Heikoin taso löytyy 2D -kasvojentunnistamisesta pelkällä etukameralla, kun taas korkein suojan taso löytyy 3D -mallinnuksen tekevistä kasvojenlukijoista (Kodituwakku 2015f, 117). Nykyään infrapunaan perustuva kasvojentunnistus alkaa olemaan järkevä vaihtoehto laitevalmistajille, koska sen valmistuskulut eivät ole niin korkeat kuin 3D -tunnistamisen omaavissa laitteissa, mutta se on paljon turvallisempi kuin pelkkään tavalliseen kameraan perustuva kasvojentunnistus (Triggs 14.1.2019).

2.2.5 Kasvojentunnistus Apple -laitteilla

Applen kehittämä Face ID -kasvojentunnistusteknologia yhdistää eri laitteistoja ja ohjelmistoja, jotka muodostavat Applen menetelmän. iPhonen etukamera tarkentaa kasvotiedot projisoimalla ja analysoimalla tuhansia infrapunapisteitä. Se luo kasvoista syvyyskartan ja tallentaa kolmiulotteisen infrapunakuvan. Applen uudemmat sirut käyttävät Applen kehittämää Neural Enginea muuntamaan nämä tiedot matemaattiseksi mallinnukseksi ja vertaamaan sitä rekisteröityihin kasvotietoihin. (Apple 22.8.2023.)

Kaikki Face ID -tiedot, mukaan lukien kasvojen matemaattiset mallinnukset, salataan ja suojataan Applen Secure Enclaven avaimella. Applen mukaan todennäköisyys huijaukselle on erittäin pieni, ja se sallii vain viisi epäonnistunutta yritystä ennen pääsykoodin vaatimista. Tietosuoja on Applelle keskeistä, joten Face ID -tiedot pysyvät ainoastaan laitteen omassa muistissa. Applen Face ID tunnistaa myös sen, että käyttäjän silmät ovat auki ja, että katse suuntautuu laitteen kameraan. Applen mukaan tämä vaikeuttaa laitteen lukituksen avaamista tietämättä. (Apple 22.8.2023.)

2.2.6 Kasvojentunnistus Windows -laitteilla

Windows 10:ssä Microsoftin kasvojentunnistus on osa yritystason henkilöllisyyden vahvistusjärjestelmää, integroituna Windows Biometric Frameworkiin (WBF) ja se tunnetaan nimellä Windows Hello. Windows Hello kasvojentunnistus käyttää lähi-infrapunakuvaukseen tarkoitettua kameraa, joka mahdollistaa Windows -laitteiden kasvojentunnistamisen. (Microsoft 15.7.2021.)

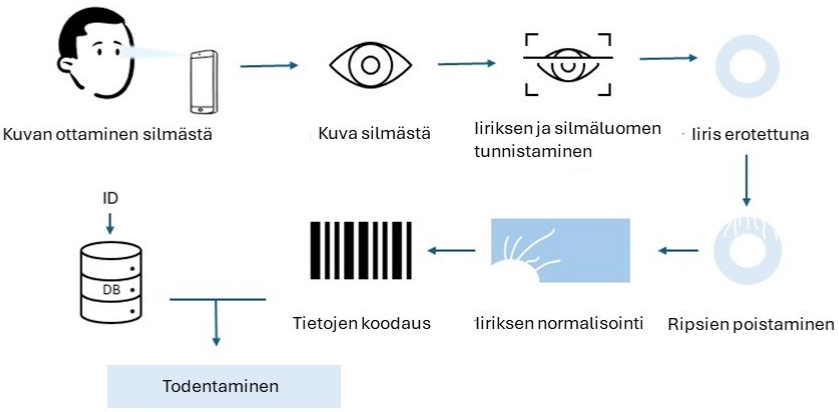
2.3 Iiristunnistin

Iiristunnistin hyödyntää silmän iiriksen ainutlaatuista rakennetta, joka eroaa yksilöllisesti väri- ja koostumusominaisuuksiltaan. Iiristunnistin käyttää harmaasävykameraa iiriksen lukemiseen. Skannaus ja analysointi kohdistuvat silmän värilliseen osaan, joka on pupillia ympäröivä alue. Iiriksen pinnan monimutkaiset yksilölliset piirteet, kuten korona, kryptat, filamentit, pisamat ja muut, mahdollistavat vertailukelpoisten tunnistetietojen erottamisen. Vaikka iiriksen kuvantaminen on suhteellisen helppoa, muuttuvat ympäristötekijät kuten valaistus ja kuvan tarkennus on huomioitava tarkasti välttääkseen mahdolliset virheet tunnistuksessa. (Kodituwakku 2015g, 118.)

2.3.1 Iiristunnistin mobiililaitteissa

Iiristunnistus ei ole enää kovinkaan yleinen tunnistusmenetelmä sen tuotantokustannusten takia. Samsung oli yksi harvoista laitevalmistajista, jotka valmistivat älypuhelimia iiristunnistimilla, mutta Samsung lopetti niiden tekemisen vuonna 2018 julkaistun Note 9 -laitteen jälkeen. (Triggs 14.1

2019.) Samsungin menetelmä (kuva 10) toimii siten, että kun käyttäjä rekisteröi silmänsä, niistä saadut tiedot tallennetaan salattuna koodina. Kun käyttäjä haluaa avata mobiililaitteensa, infrapunavalo ja silmäkamera toimivat yhdessä tallentaakseen iiriksen kuviot tunnistamista varten, erottavat ja digitalisoivat kuviot ja vertaavat digitalisoitua kuvioita tallennettuun koodiin varmistaakseen pääsyn laitteelle. (Samsung 4.8.2016.)



Kuva 8. Iiristunnistamisen tapahtumaketju (mukaillen Samsung 4.8.2017)

Iiristunnistimen kanssa on ollut myös ongelmia. Samsungin vuonna 2017 julkaiseman Galaxy S8 älypuhelimen iiristunnistin onnistuttiin murtamaan vain kuukausi sen julkaisun jälkeen. Saksalaiset hakkerit käyttivät murtamiseen kuvaa silmästä ja piilolinssiä saavuttaakseen silmän kaarevuuden. (Hern 23.5.2017.)

2.4 Biometristen tunnistusmenetelmien yleiset tietoturvariskit ja ongelmat yksityiskäyttäjille

Kaikissa edellisissä luvuissa läpi käydyissä biometrisissä tunnistusmenetelmissä on paljon hyviä puolia, kuten niiden helppokäyttöisyys, mutta jokaiseen liittyy silti isoja riskejä tietoturvan näkökulmasta. Tässä luvussa käydään läpi yleisimmät riskit yksityiskäyttäjille.

Google varoittaa, että katsomalla älypuhelinta sopivasta kulmasta, voi sen lukituksen avata, vaikka se ei olisi tarkoitus (Google s.a. b). Tämä mahdollistaa älypuhelimen avauksen vahingossa, mikä ei onnistuisi helposti, jos älypuhelin pitäisi avata perinteisellä PIN-koodilla tai salasanalla. Myös joku muu voi avata älypuhelimesi lukituksen, jos se pidetään kasvojasi vasten (Google s.a. b). Täten nukkuvan tai tiedottoman ihmisen laitteet ovat vaarassa luvattomalle käytölle. Sama vaara on myös yleisimmissä käytössä olevissa sormenjälkitunnistimissa.

Sekä Android, iOS sekä Windows -käyttöjärjestelmät vaativat biometrisen tunnistautumisen kanssa, joko salasanaa, PIN-koodia tai suojakuvioita (Google s.a. b; Apple support 22.8.2023; Microsoft 11.5.2020). Tämä on hieman ristiriitaista, koska tällöin biometristen tunnistusmenetelmien luoma suoja menettää merkityksensä, jos laitteille voi päästä sisään käyttäen mahdollisesti perinteistä salasanaa tai PIN-koodia ja näin kokonaan ”ohittaa” biometrinen tunnistusmenetelmä ja sen luoma lisäsuoja.

Biometrinen tunnistusmenetelmä voi epäonnistua tunnistustapahtumassa monesta eri syystä. Sormenjälkitunnistimien kanssa ongelmina ovat likaiset, märät tai liian kuivat sormet. Myös liian kirkas auringonvalo tai näytönsuojan käyttäminen voi aiheuttaa ongelmia (Google s.a. c). Kasvojentunnistimen kanssa ongelmiksi voi muodostua liian huonot valaistusolosuhteet, kuten liika kirkkaus tai pimeys. Aurinko- tai silmälasit voivat myös aiheuttaa tunnistuksen epäonnistumista. Lisäksi muun muassa meikkaaminen tai päähineet voivat aiheuttaa hankaluuksia tunnistamisessa. (Google s.a. b.)

2.5 Aiempaa tutkimusta aiheesta

Entrust Cybersecurity -instituutti on tehnyt maailmanlaajuisen kyselyn 1 450 kuluttajalle, jotka olivat yli 18-vuotiaita, koskien heidän käyttäytymistään ja asenteistaan suosittuja identiteettiratkaisuja, kuten biometristä tunnistautumista kohtaan. Kysely on tehty verkossa käytettävän kyselyalustan avulla 8. joulukuuta ja 16. joulukuuta 2022 välisenä aikana. Kyselyn tuloksista on havaittu, että 33 % kuluttajista on käyttänyt biometristä tunnistusmenetelmää aina salasanan sijaan. Yhteensä 75 % kyselyn vastaajista on käyttänyt biometrisiä tunnistusmenetelmiä säännöllisesti, kun taas vain 16 % vastaajista ei ollut käyttänyt biometrisiä tunnistusmenetelmiä ollenkaan. Kyselyyn vastaajien keskuudessa 53 % on pitänyt sormenjälkitunnistinta turvallisempana kuin salasanaa ja 46 % vastaajista on pitänyt kasvojentunnistinta turvallisempana kuin salasanaa. (Entrust Cybersecurity Institute 2023, 2, 3, 9.)

Rauramo on tutkinut aihetta vuoden 2018 opinnäytetyössään ”Tunnistusmenetelmät yksityiskäyttäjän näkökulmasta”. Tutkimuksessa esitettiin yleistä tietoa tunnistusmenetelmistä ja tehtiin kysely,

jossa selvitettiin 47 vastaajan kokemuksia ja mielipiteitä erinäisistä tunnistusmenetelmistä. (Rauramo 2018, 1.) Kyselyn tuloksista on havaittu, että biometriset tunnistusmenetelmät eivät olleet vielä kovinkaan suuressa käytössä vastaajien kesken, mutta niiden käytön on arvioitu lisääntyvän tulevaisuudessa (Rauramo 2018, 22 ,27, 29).

Mäki taas on tutkinut aiheitta vuoden 2020 opinnäytetyössään ”Mobiililaitteiden sormenjälkitunnistaminen”. Tutkimuksessa on keskitytty ainoastaan sormenjälkitunnistimeen ja sen toimintaan ja riskeihin. Tutkimuksessa on käyty läpi myös sen aikaista laitekantaa ja suoritettu kolme asiantuntijahaastattelua. (Mäki 2020, 1.)

Asiantuntijahaastatteluiden tuloksista on käynyt ilmi, että sormenjälkilukijaa on pidetty turvallisena tapana ja, että sen toimivuus ja käyttökokemus on ollut hyvällä tasolla (Mäki 2020, 18, 20). Asiantuntijoista kaksi ovat olleet sitä, mieltä, että sormenjälkilukijat pysyvät vielä pitkään tapana tunnistautua ja niiden kehittyvän. Kolmas asiantuntija on ollut taas sitä mieltä, että hän ei halunnut ajatella sormenjälkitunnistautumista tulevaisuuden tunnistusmenetelmänä, koska hän ei luottanut laitevalmistajien pitävän kiinni biometristen tietojen vastuullisista käyttötavoista. (Mäki 2020, 21.)

3 Tutkimus

Tutkimuksen kyselyosuus toteutettiin nimettömänä vastattavana kyselytutkimuksena. Nimettömyyteen päädyttiin, koska näin tutkimukselle ei tarvinnut hakea erillistä tutkimuslupaa. Kyselyn kysymykset kattoivat seuraavat osa-alueet: Käyttäjien kokemukset ja preferenssit biometrisistä tunnistusmenetelmistä, koettu tietoturva biometristen tunnistusmenetelmien käytöstä ja mahdolliset ongelmatilanteet. Seuraavaksi esitellään valitut tutkimusmenetelmät ja itse tutkimuksen toteutus. Kyselylomake löytyy liitteenä opinnäytetyön lopussa.

3.1 Tutkimuseettiset käytännöt

Tutkimuksessa aion sitoutua tutkimuseettisen neuvottelukunnan 2012 julkaisemaan ohjeeseen: Hyvä tieteellinen käytäntö (TENK 2012). Myös Haaga-Helia ammattikorkeakoulun eettinen ohjeistus on otettu huomioon (Haaga-Helia 2023). Kyselyssä ei tallenneta vastaajien henkilötietoja.

3.2 Tutkimusmenetelmä

Opinnäytetyössäni tutkin aluksi yleisimpiä biometrisiä tunnistusmenetelmiä mobiililaitteissa tekemällä kirjallisuuskatsauksen. Tämä osuus löytyy opinnäytetyöni luvusta kaksi. Valitsin kirjallisuuskatsauksen tutkimusmenetelmäksi, koska sen avulla pystyin avaamaan tehokkaasti mobiililaitteiden biometristen tunnistusmenetelmien laajaa kirjoa, sekä linkittää sen sisältämää tietoa kyselystä saatuihin tuloksiin. Kirjallisuuskatsauksen avulla kerätyt tiedot ovat suurimmalta osalta yleisluonteisia ja toimivat pohjan kyselytutkimukselle. Kirjallisuuskatsauksen tiedot pohjautuivat luotettaviin lähteisiin, kuten tutkimuksiin, kirjoihin, tietokantoihin sekä verkkosivuihin.

Pääpaino tutkimuksessani oli kerätä mittaavaa dataa ihmisten kokemuksista mobiililaitteiden biometrisistä tunnistusmenetelmistä. Tähän tarkoitukseen tutkimusmenetelmäksi valittiin kvantitatiivinen eli määrällinen tutkimus. Määrällistä tutkimusta voi nimittää myös tilastolliseksi tutkimukseksi, koska sen avulla selvitetään prosenttiosuuksiin ja lukumääriin liittyviä kysymyksiä (Heikkilä 2014, 15). Tutkimuksessa haluttiin mitata mahdollisimman suuren joukon kokemuksia ja mielipiteitä biometrisistä tunnistusmenetelmistä.

Tehdyn tutkimuksen kysely koostui strukturoiduista vaihtoehto- sekä mielipidekysymyksistä (Heikkilä 2014, 15). Tutkimuslomakkeen samaa aihetta koskevat kysymykset oli ryhmitelty omiksi loogisiksi kokonaisuuksiksi. Lomake testattiin myös useaan kertaan ja muokattiin saadun palautteen perusteella ennen sen lähettämistä vastaajille. (Heikkilä 2014, 47.)

Tutkimuksen perusjoukko eli vastaajat saatiin osatutkimuksella eli otantatutkimuksella. Perusjoukkona olivat Suomessa asuvat mobiililaitteita käyttävät yksityiskäyttäjät. Koska mahdollisuutta tutkia koko perusjoukkoa ei ollut, niin tällöin vai tietyn perusjoukon osajoukko eli otos tutkitaan (Heikkilä 2014, 12, 13). Tutkimuksen osajoukkona olivat Helsingin kaupunginkirjasto Oodin työntekijät ja opinnäytetyön tekijän laajaan lähipiiriin kuuluvia henkilöitä. Koska kysely lähetettiin vain näille ryhmille, se muodostaa otoksen perusjoukosta, mutta koko perusjoukkoa ei ole tavoiteltu. Tarkemmin määriteltynä kyseessä oli harkinnanvarainen näyte, koska tutkittavat valittiin muulla tavalla kuin täysin sattumaa hyödyntäen (Heikkilä 2014, 39).

3.3 Tutkimuksen toteutus

Tutkimus toteutettiin survey eli kyselytutkimuksena. Tähän toteutukseen päädyttiin, koska näin saatoin saada mahdollisimman suuren vastaajamäärän nopealla aikataululla. Linkki kyselyyn lähettiin WhatsApp -viestintäsovelluksen kautta Helsingin kaupunginkirjasto Oodin työntekijöiden omaan viestiryhmään, sekä muihin viestiryhmiin, jotka koostuivat ystävistäni ja heidän ystävistään. Tutkimuslomake laadittiin Google Forms -palvelulla aiemman osaamisen ja tästä johtuvan helppokäyttöisyyden takia. Myös Google Formsin automaattisesti luomia kuvaajia käytettiin tulosten analysoimisessa ja itse tulosten visuaalisessa esittelyssä. Kyselyyn pystyi vastaamaan aikavälillä 8.3.-24.3.2024. Kyselystä kerätty tutkimusaineisto analysoitiin määrällisin menetelmin, koska kyseessä on kyselytutkimus.

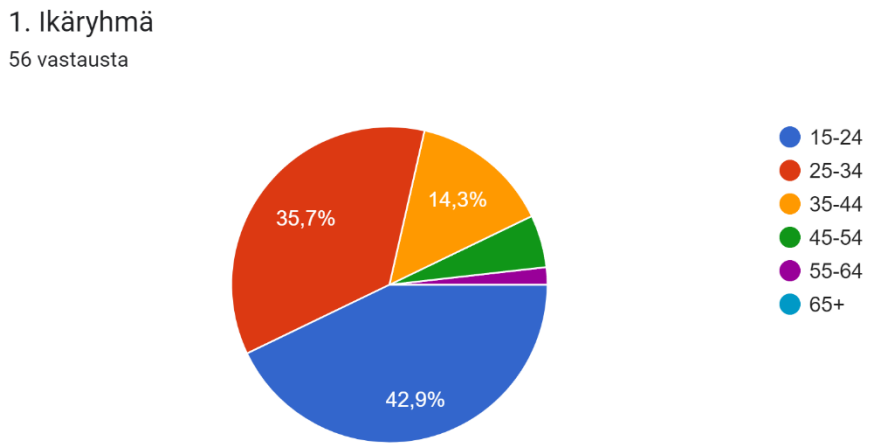
4 Tulokset

Tässä luvussa käydään läpi kyselyn tulokset ja ne on ryhmitelty tutkimusongelmien mukaan omiin ryhmiinsä. Kyselyyn osallistui yhteensä 56 vastaajaa. Seuraavaksi tulevassa alaluvussa esitellään vastaajien taustatietoja. Lukijalle tiedoksi se, että ensimmäisenä tekstissä tulee kysymyksen tulokset, jonka jälkeen on aina sen alapuolella siihen liittyvä kuvio.

4.1 Vastaajien taustatiedot

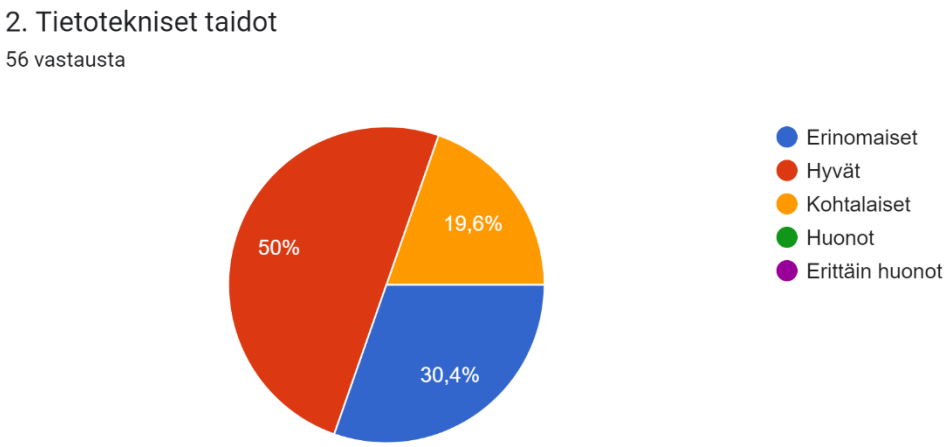
Kyselyn kolme ensimmäistä kysymystä kartoitti vastaajien taustatietoja. Ensimmäisessä kysymyksessä kartoitettiin vastaajien ikäryhmiä, toisessa tietoteknisiä taitoja ja kolmannessa vastaajien laitteiden käyttöjärjestelmiä.

Kuten kuviosta 1 näkee, vastaajien iässä oli haettua variaatiota. Vastaajista 42,9 % oli 15–24-vuotiaita, kun taas toiseksi suurin ikäryhmä oli 25–34-vuotiaat, joita oli 35,7 %. 35–44-vuotiaita vastaajia oli 14,3 %. Vastaajista 45–54-vuotiaita oli ainoastaan kolme eli 5,4 % ja 55–64-vuotiaita vastaajia oli vain yksi eli 1,8 %. Yli 65-vuotiaita vastaajia ei ollut yhtään.



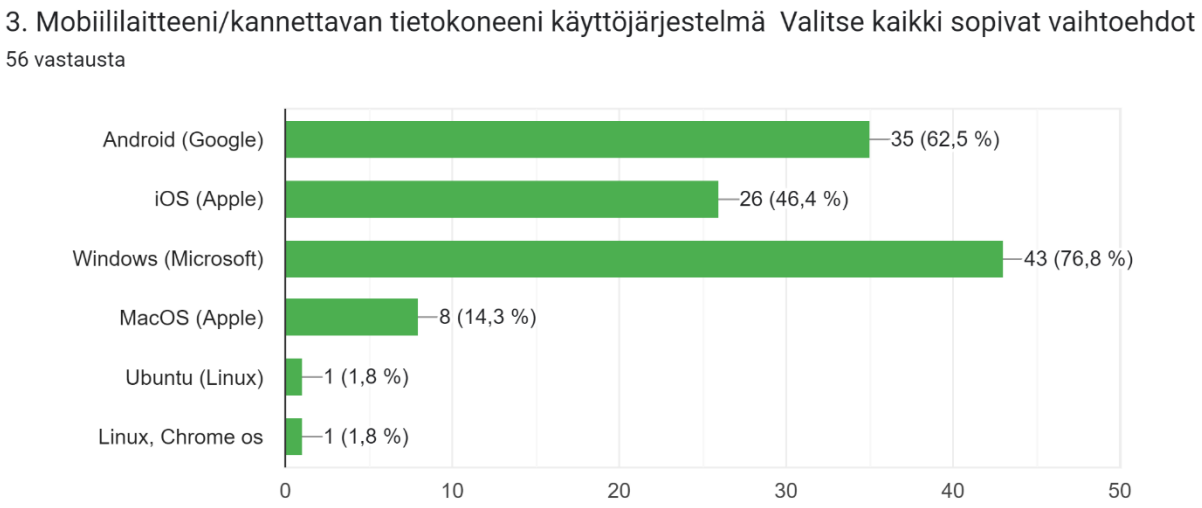
Kuvio 1. Vastaajien ikäryhmät

Toisessa kysymyksessä kartoitettiin vastaajien tietoteknisiä taitoja. Kuten kuviosta 2 voidaan huomata, puolet vastaajista eli 50 % koki omien tietoteknisten taitojen olevan hyvällä tasolla. 30,4 % vastaajista arvioi omat tietotekniset taidot erinomaisiksi. 19,6 % vastaajista taas koki tietoteknisten taitojen olevan kohtalaiset. Kukaan vastaajista ei vastannut tietoteknisten taitojen olevan huonot tai erittäin huonot.



Kuvio 2. Vastaajien tietotekniset taidot

Viimeisessä taustatietoja kysyvässä kysymyksessä kartoitettiin vastaajien mobiililaitteiden käyttöjärjestelmää. Kysymykseen oli mahdollista vastata monta valintaa, sekä lisätä oma vaihtoehto. Kuviosta 3 käy ilmi, että älypuhelimien käyttöjärjestelmistä Googlen kehittämä Android oli suosituin ja yhteensä 62,5 % vastasi käyttävän sitä. Applen iOS -käyttöjärjestelmää käytti 46,4 % vastaajista. Kannettavien tietokoneiden käyttöjärjestelmistä Microsoftin Windowsia käytti 76,8 % vastaajista. 14,3 % vastaajista käytti Applen MacOS -käyttöjärjestelmää kannettavassa tietokoneessaan. Kaksi vastaajaa lisäsi oman vaihtoehdon ja he käyttivät Linux -pohjaisia Ubuntua ja Chrome OS -käyttöjärjestelmiä kannettavissaan.

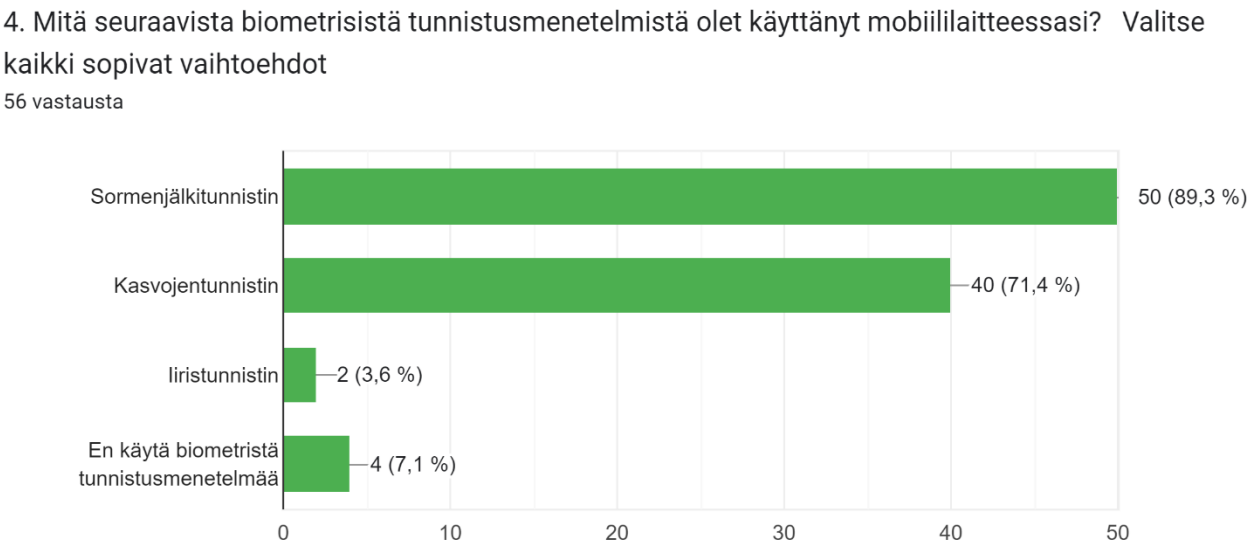


Kuvio 3. Vastaajien mobiililaitteiden käyttöjärjestelmät

4.2 Suosivatko yksityiskäyttäjät sormenjälki-, kasvojen- vai iiristunnistinta biometrisistä tunnistusmenetelmistä

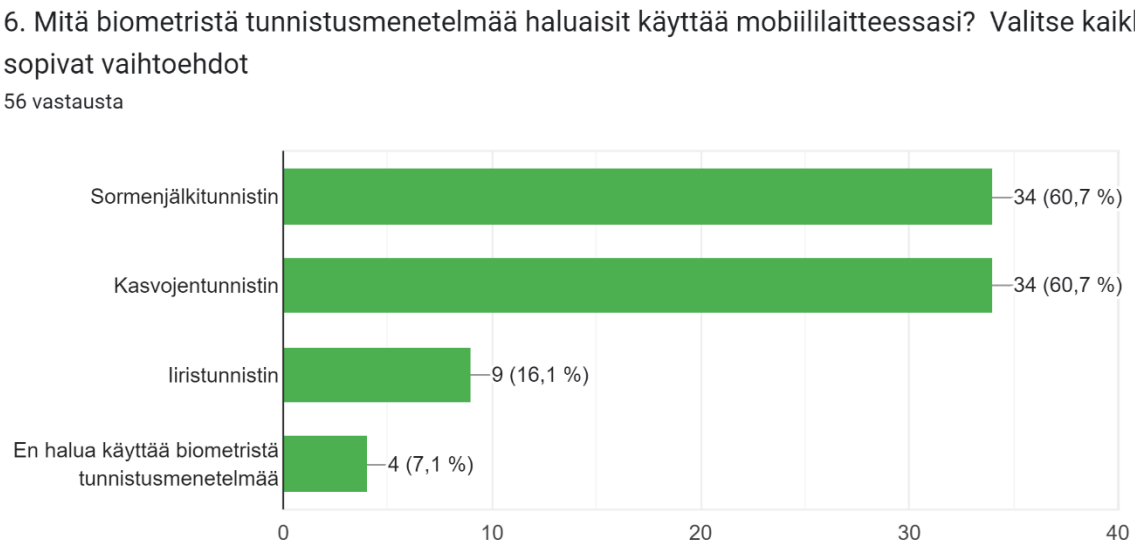
Seuraavissa kysymyksissä kartoitettiin, mitkä biometriset tunnistusmenetelmät olivat käyttäjien suosiossa, sekä selvitettiin, mihin teknologioihin vastaajien biometriset tunnistusmenetelmät perustuivat.

Kysymykseen oli mahdollista valita monta vaihtoehtoa. Vastaajista vain neljä eli 7,1 % ei käyttänyt biometristä tunnistusmenetelmää. Loput 92,9 % vastaajista käytti joko sormenjälki-, kasvojen- tai iiristunnistinta. Vastaajista 89,3 % käytti sormenjälkitunnistinta ja 71,4 % kasvojentunnistinta. Iristunnistinta käytti ainoastaan kaksi vastaajaa eli 3,6 %. (Kuvio 4.)



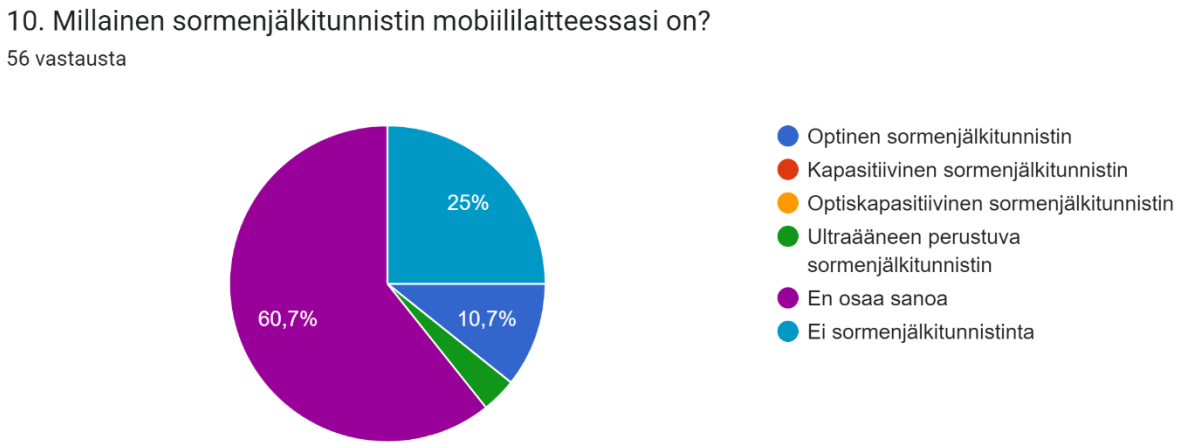
Kuvio 4. Biometristen tunnistusmenetelmien suosio

Kysymykseen oli mahdollista valita monta vaihtoehtoa. Vastaajista 60,7 % halusi käyttää sormenjälkitunnistinta ja kasvojentunnistinta. 16,1 % halusi käyttää iiristunnistinta. Vain 7,1 % vastaajista ei halunnut käyttää mitään biometristä tunnistusmenetelmää. (Kuvio 5.)



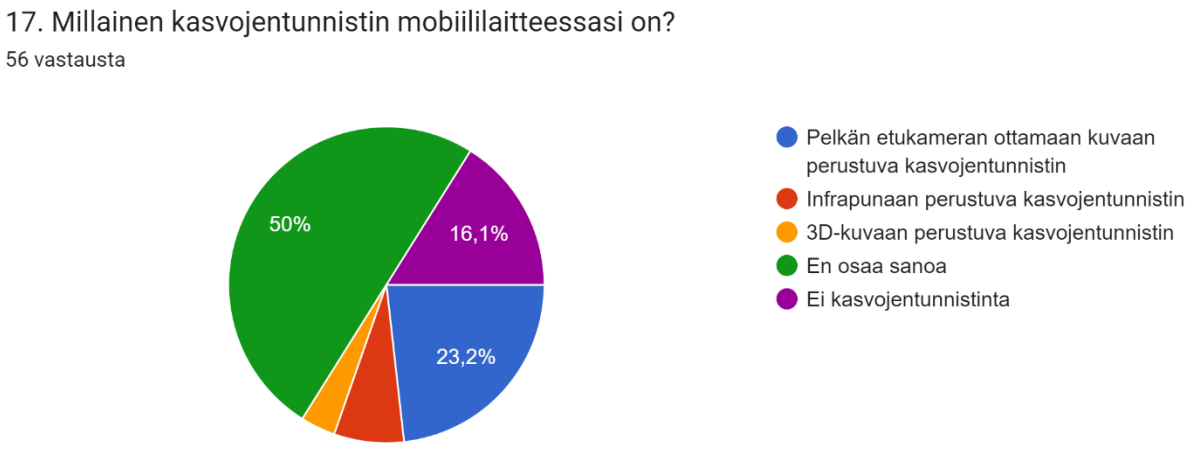
Kuvio 5. Kiinnostus biometrisiä tunnistusmenetelmiä kohtaan

Vastaajista suuri osa (60,7 %), ei osannut sanoa minkälainen sormenjälkitunnistin heidän mobiililaitteessaan oli. 25 % vastaajista ei omistanut mobiililaitetta sormenjälkitunnistimella. 10,7 % vastaajista tunnisti mobiililaitteessaan olevan optinen sormenjälkitunnistin, kun taas vain kaksi vastaajaa eli 3,6 % tunnisti laitteensa sormenjälkitunnistimen perustuvan ultraääneen. (Kuvio 6.)



Kuvio 6. Sormenjälkitunnistimen tyyppi

Puolet vastaajista eli 50 % ei osannut sanoa millainen kasvojentunnistin heidän mobiililaitteessaan oli. 23,2 % vastaajista vastasi mobiililaitteessaan olevan pelkän etukameran ottamaan kuvaan perustuva kasvojentunnistin. Infrapunaan perustuvan kasvojentunnistimen omasi 7,1 % vastaajista. 3,6 % vastaajista vastasi mobiililaitteessaan olevan 3D-kuvaan perustuva kasvojentunnistin. Vastaajien keskuudesta 16,1 % ei omistanut mobiililaitetta kasvojentunnistimella. (Kuvio 7.)

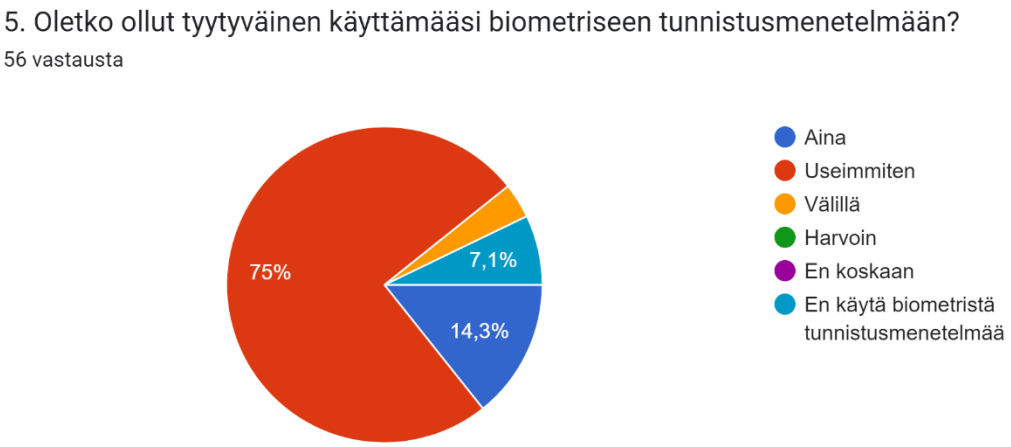


Kuvio 7. Kasvojentunnistimen tyyppi

4.3 Millaisia kokemuksia kuluttajilla on biometrisiin tunnistusmenetelmiin liittyen

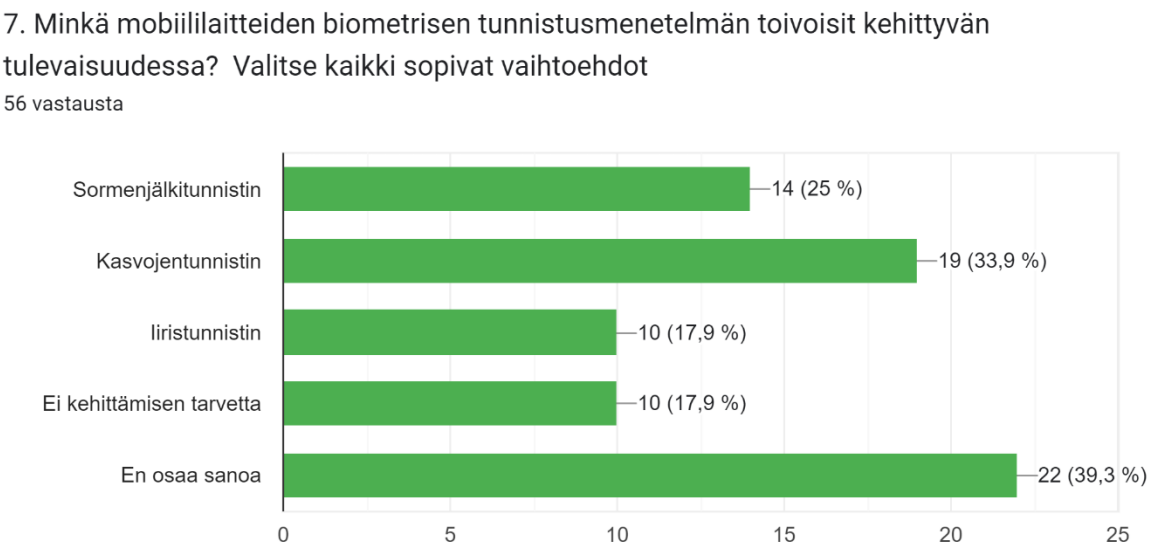
Seuraavat kysymykset koskivat kuluttajien kokemuksia eri biometrisiin tunnistusmenetelmiin. Kysymyksissä keskityttiin muun muassa kokemuksiin käytettävyydestä ja tietoturvasta. Lisäksi selvitettiin tietoja biometristen tunnistusmenetelmien yleisistä käyttötarkoituksista.

75 % vastaajista oli useimmiten tyytyväinen käyttämäänsä biometriseen tunnistusmenetelmään. 14,3 % vastaajista koki olevansa aina tyytyväinen niiden toimintaan. 7,1 % vastaajista ei käyttänyt biometristä tunnistusmenetelmää. 3,6 % vastaajista koki olevansa vain välillä tyytyväisiä biometriseen tunnistusmenetelmään. (Kuvio 8.)



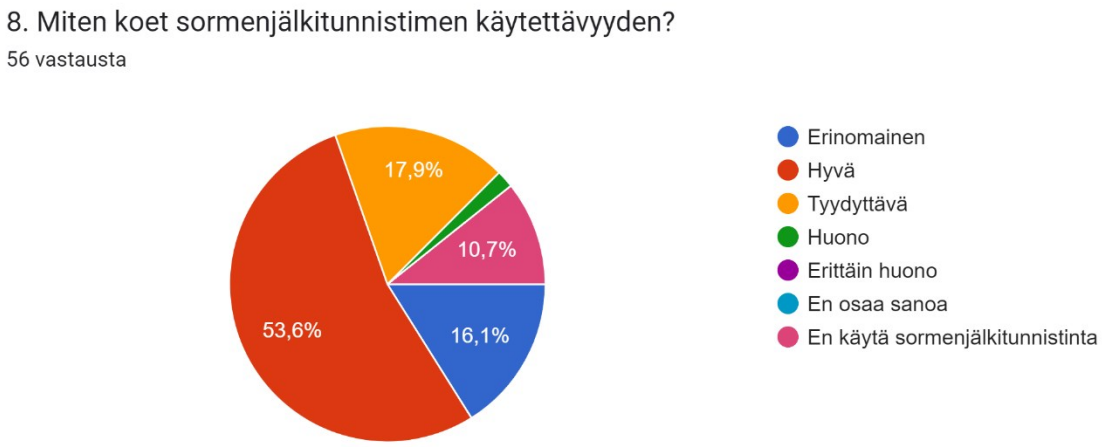
Kuvio 8. Tyytyväisyys biometrisiä tunnistusmenetelmiä kohtaan

Kysymykseen oli mahdollista valita monta vaihtoehtoa. 39,3 % vastaajista ei osannut sanoa, minkä biometrisen tunnistusmenetelmän he toivoisivat kehittyvän tulevaisuudessa. Kuitenkin 33,9 % toivoi kasvojentunnistimen kehityttävän ja 25 % toivoi sormenjälkitunnistimen kehittyvän. 17,9 % vastaajista toivoi iiristunnistimen kehittyvän ja 17,9 % vastaajista ei kokenut mitään kehittämisen tarvetta biometrisiin tunnistusmenetelmiin. (Kuvio 9.)



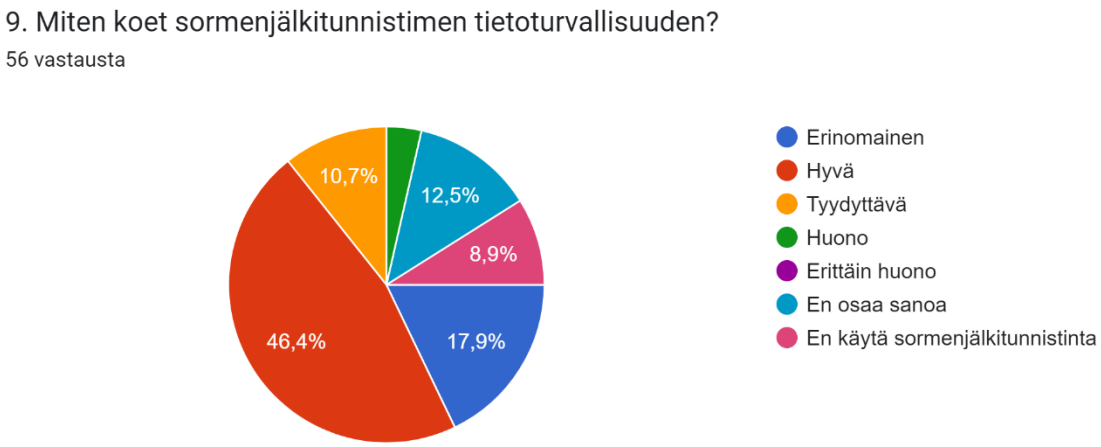
Kuvio 9. Biometristen tunnistusmenetelmien kehittyminen tulevaisuudessa

Yli puolet vastaajista (53,6 %) koki sormenjälkitunnistimen käytettävyyden olevan hyvällä tasolla. 17,9 % vastaajista koki käytettävyyden olevan tyydyttävällä tasolla. Erinomaiseksi sormenjälkitunnistimen käytettävyyden koki 16,1 % vastaajista. 10,7 % vastaajista ei käyttänyt sormenjälkitunnistinta. 1,8 % eli vain yksi vastaaja koki sormenjälkitunnistimen käytettävyyden olevan huono. (Kuvio 10.)



Kuvio 10. Sormenjälkitunnistimen käytettävyys

46,4 % vastaajista koki sormenjälkitunnistimen tietoturvallisuuden olevan hyvällä tasolla. 17,9 % vastaajista koki sormenjälkitunnistimen tietoturvallisuuden olevan erinomainen, kun taas 12,5 % vastaajista ei osannut sanoa, miten he kokivat sormenjälkitunnistimen tietoturvallisuuden. 10,7 % vastaajista koki sormenjälkitunnistimen tietoturvallisuuden olevan tyydyttävä ja 3,6 % koki tietoturvallisuuden olevan huono. 8,9 % vastaajista ei käyttänyt sormenjälkitunnistinta. (Kuvio 11.)



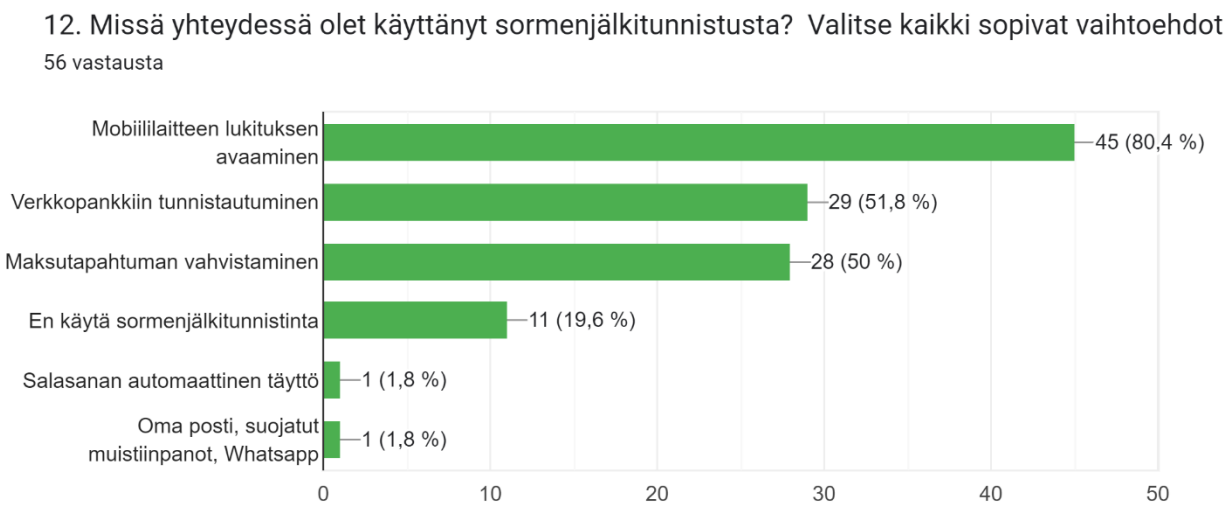
Kuvio 11. Sormenjälkitunnistimen tietoturvallisuus

58,9 % vastaajista oli lisännyt laitteellensa 1–2 sormenjälkeä. 25 % vastaajista eivät olleet lisänneet laitteellensa yhtään sormenjälkeä. 16,1 % vastaajista oli lisännyt laitteellensa 3–5 sormenjälkeä. (Kuvio 12.)

Kuvio 12. Sormenjälkien lisääminen laitteille

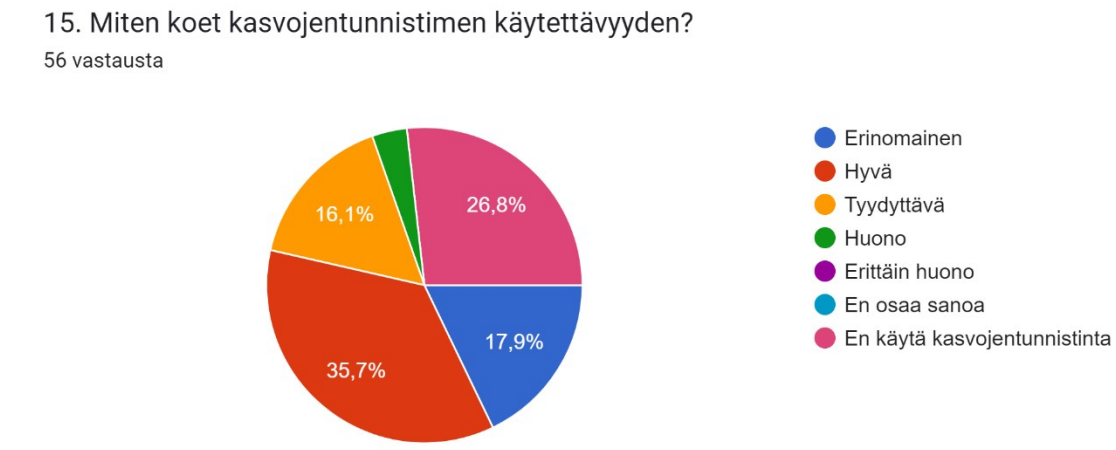
Kysymykseen oli mahdollista valita monta vaihtoehtoa. 80,4 % vastaajista oli käyttänyt sormenjälkitunnistusta mobiililaitteensa lukituksen avaamiseen, kun taas 51,8 % vastaajista oli käyttänyt sormenjälkitunnistusta verkkopankkiin tunnistautumisessa ja 50 % vastaajista maksutapahtuman vahvistamiseen. 19,6 % vastaajista ei käyttänyt sormenjälkitunnistinta. Muu -vaihtoehtona vastauksina

tuli, että sormenjälkitunnistusta käytettiin salasanan automaattiseen täyttöön, oma postiin, suojattuihin muistiinpanoihin ja WhatsAppiin. (Kuvio 13.)



Kuvio 13. Sormenjälkitunnistimen käyttäminen

Vastaajista 35,7 % koki kasvojentunnistimen käytettävyyden olevan hyvä. 26,8 % vastaajista ei käyttänyt kasvojentunnistinta. 17,9 % vastaajista koki kasvojentunnistimen käytettävyyden olevan erinomainen. 16,1 % vastaajista koki käytettävyyden tyydyttäväksi. 3,6 % vastaajista koki käytettävyyden olevan huono. (Kuvio 14.)

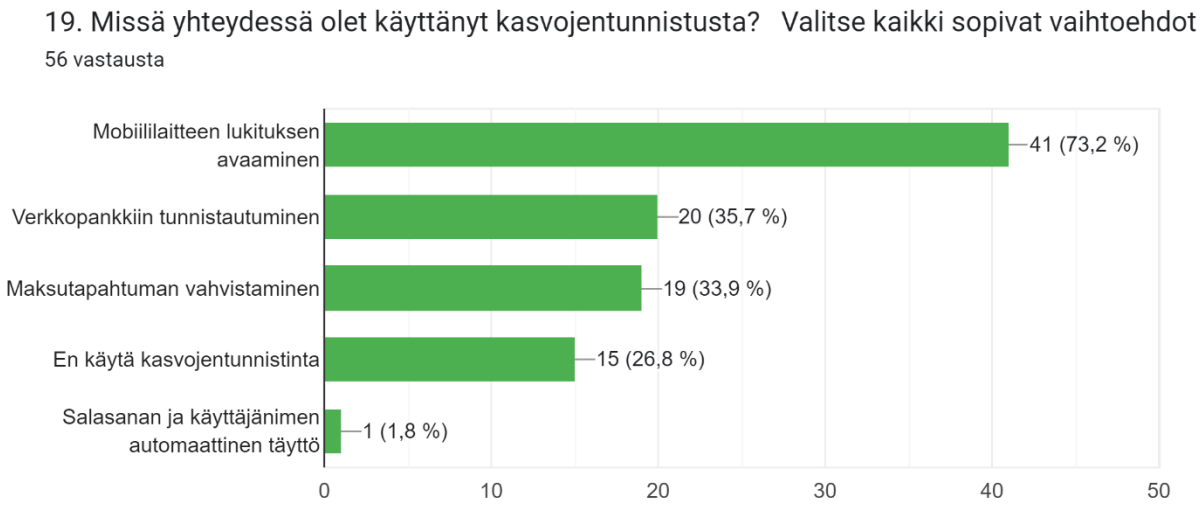


Kuvio 14. Kasvojentunnistimen käytettävyys

26,8 % vastaajista koki kasvojentunnistimen tietoturvallisuuden olevan tyydyttävä. 25 % vastaajista ei käyttänyt kasvojentunnistinta. 23,2 % vastaajista koki tietoturvallisuuden olevan hyvällä tasolla kasvojentunnistimessa. Erinomaiseksi kasvojentunnistimen tietoturvallisuuden koki 12,5 % vastaajista. 5,4 % vastaajista koki kasvojentunnistimen tietoturvallisuuden huonoksi. 5,4 % vastaajista ei osannut sanoa, miten he kokivat kasvojentunnistimen tietoturvallisuuden. 1,8 % eli yksi vastaaja koki kasvojentunnistimen tietoturvallisuuden olevan erittäin huono. (Kuvio 15.)

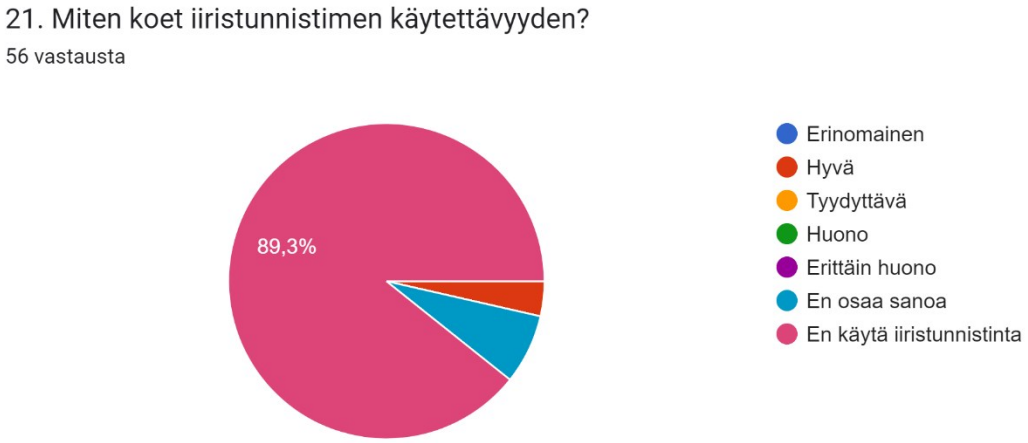
Kuvio 15. Kasvojentunnistimen tietoturvallisuus

Kysymykseen oli mahdollista valita monta vaihtoehtoa. 73,2 % vastaajista oli käyttänyt kasvojentunnistusta mobiililaitteen lukituksen avaamiseen, kun taas 35,7 % vastaajista oli käyttänyt kasvojentunnistusta verkkopankkiin tunnistautumisessa ja 33,9 % vastaajista maksutapahtuman vahvistamiseen. 26,8 % vastaajista ei käyttänyt kasvojentunnistusta. Muu -vaihtoehtona vastauksina tuli, että kasvojentunnistusta käytettiin salasanan ja käyttäjänimen automaattiseen täyttöön. (Kuvio 16.)



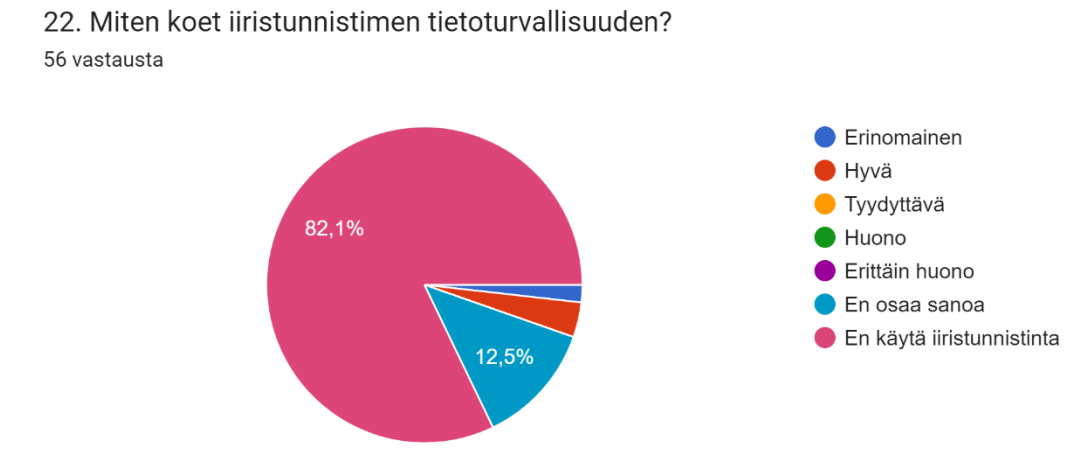
Kuvio 16. Kasvojentunnistimen käyttäminen

89,3 % vastaajista ei käyttänyt iiristunnistinta. 7,1 % vastaajista ei osannut sanoa kokemustaan iiristunnistimen käytettävyyteen. 3,6 % vastaajista koki iiristunnistimen käytettävyyden olevan hyvä. (Kuvio 17.)



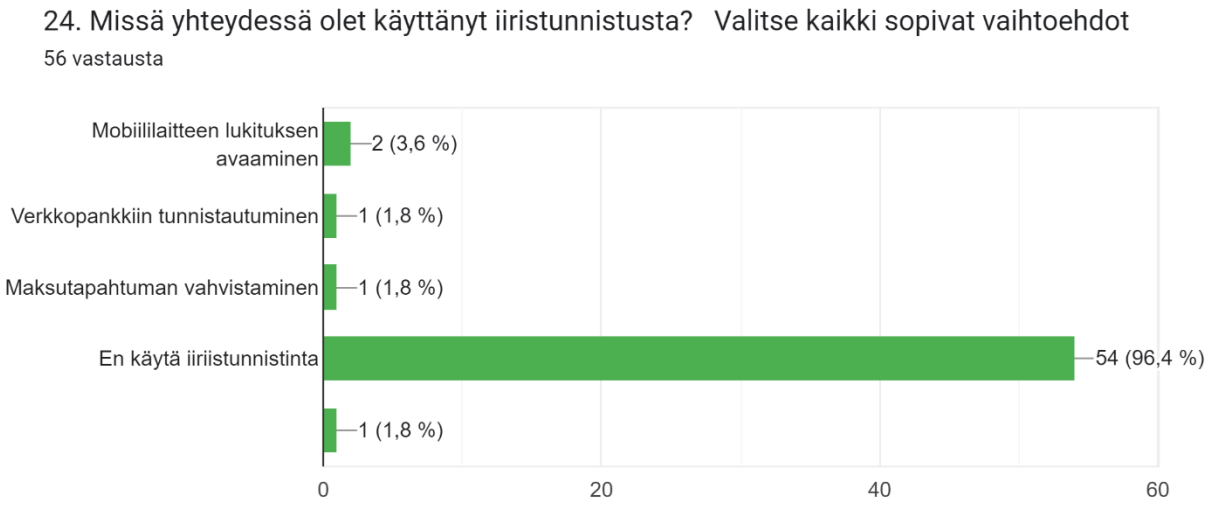
Kuvio 17. Iiristunnistimen käytettävyys

82,1 % vastaajista ei käyttänyt iiristunnistinta. 12,5 % vastaajista ei osannut sanoa kokemustaan iiristunnistimen tietoturvallisuuteen. 3,6 % vastaajista koki iiristunnistimen tietoturvan olevan hyvä, kun taas 1,8 % vastaajista koki iiristunnistimen tietoturvallisuuden erinomaiseksi. (Kuvio 18.)



Kuvio 18. Iiristunnistimen tietoturvallisuus

Kysymykseen oli mahdollista valita monta vaihtoehtoa. 96,4 % vastaajista ei käyttänyt iiristunnistinta missään kysymyksessä mainituissa yhteyksissä. Mobiililaitteen lukituksen avaamiseen vastaajista 3,6 % oli käyttänyt iiristunnistinta. 1,8 % vastaajista oli käyttänyt iiristunnistinta verkkopankkiin tunnistautumisessa ja 1,8 % vastaajista maksutapahtuman vahvistamiseen. Muu -vaihtoehtona tuli yksi vastaus, mutta sitä ei ollut tarkennettu. (Kuvio 19.)

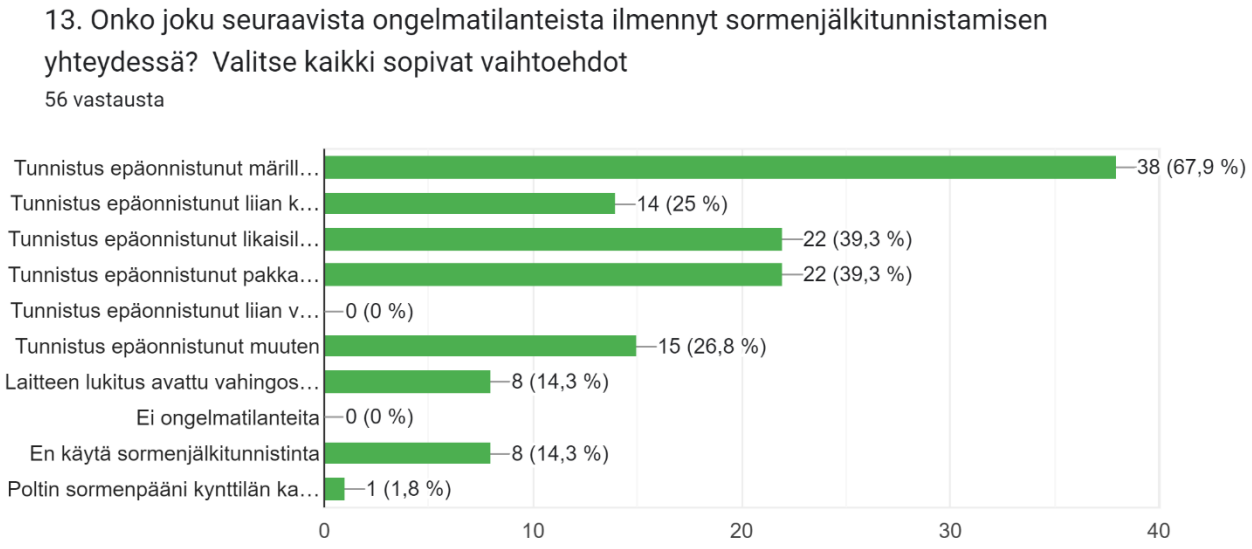


Kuvio 19. Iiristunnistimen käyttäminen.

4.4 Mitä haasteita yksityiskäyttäjät ovat kohdanneet biometrisiin tunnistusmenetelmiin liittyen

Seuraavat kysymykset koskivat biometrisiin tunnistusmenetelmiin liittyviin haasteisiin. Kysymyksissä keskityttiin selvittämään, mitä yleisiä ongelmatilanteita ilmenee eri biometristen tunnistusmenetelmien kanssa. Lisäksi vastaajilta kysyttiin siitä, onko joku ulkopuolinen päässyt heidän laitteelleen biometrisestä tunnistusmenetelmästä huolimatta.

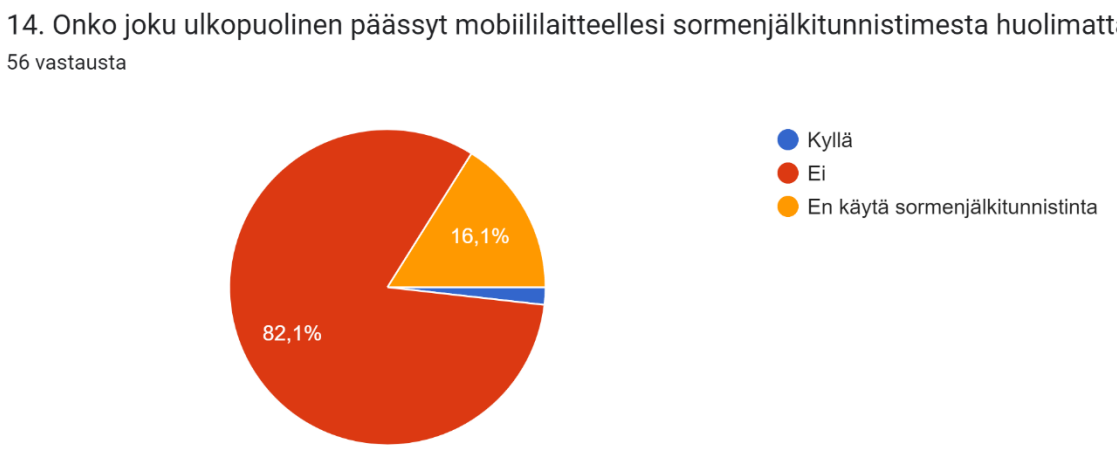
Kysymykseen oli mahdollista valita monta vaihtoehtoa. 67,9 % vastaajista oli kohdannut sormenjälkitunnistuksen epäonnistumista märillä käsillä. 39,3 % vastaajista tunnistus oli epäonnistunut likaisilla käsillä sekä pakkasella. 26,8 % vastaajista tunnistus oli epäonnistunut muuten. Liian kuivilla käsillä tunnistus oli epäonnistunut 25 % vastaajista. Laitteen lukitus oli avautunut vahingossa 14,3 % vastaajista. 14,3 % vastaajista ei käyttänyt sormenjälkitunnistusta. Muu -vaihtoehto kohtaan vastattiin, että tunnistus oli epäonnistunut sormeen kohdistuneen palovamman takia. Kenenkään vastaajan sormenjälkitunnistus ei ollut epäonnistunut liian valoissa. Ongelmatilanteita oli ilmennyt kaikilla sormenjälkitunnistusta käyttävillä. (Kuvio 20.)



Kuvio 20. Sormenjälkitunnistimen ongelmatilanteita

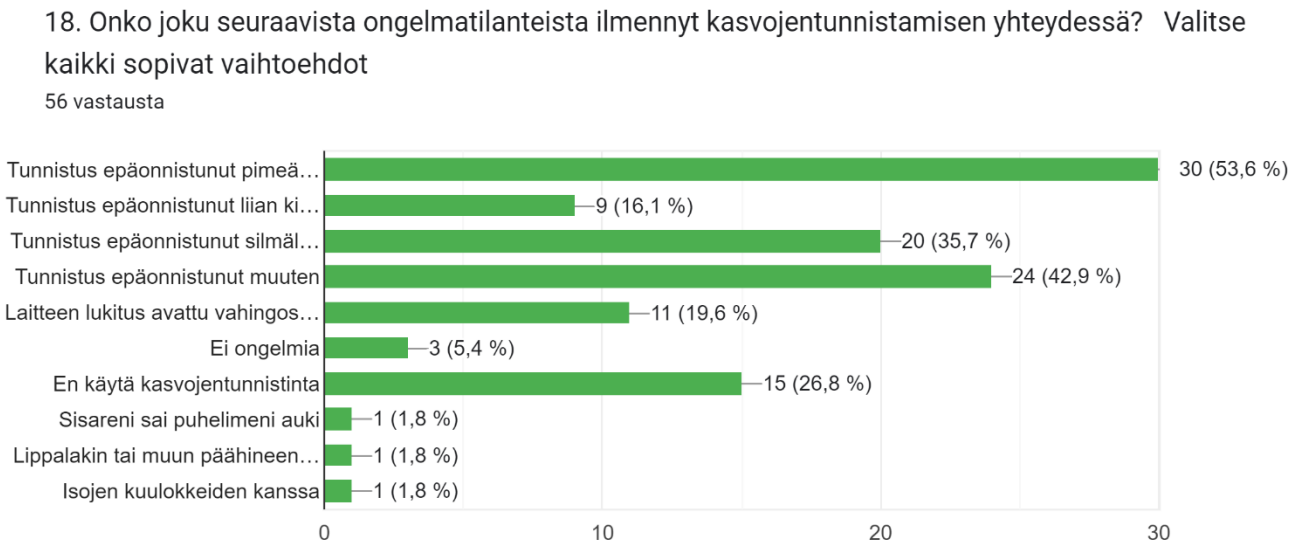
82,1 % vastaajista vastasivat, että kukaan ulkopuolinen ei ollut päässyt heidän laitteelleen sormenjälkitunnistuksen kanssa. 16,1 % vastaajista ei käyttänyt sormenjälkitunnistusta. 1,8 % eli yksi

vastasi, että ulkopuolinen oli päässyt hänen laitteelleen sormenjälkitunnistuksesta huolimatta. (Kuvio 21.)



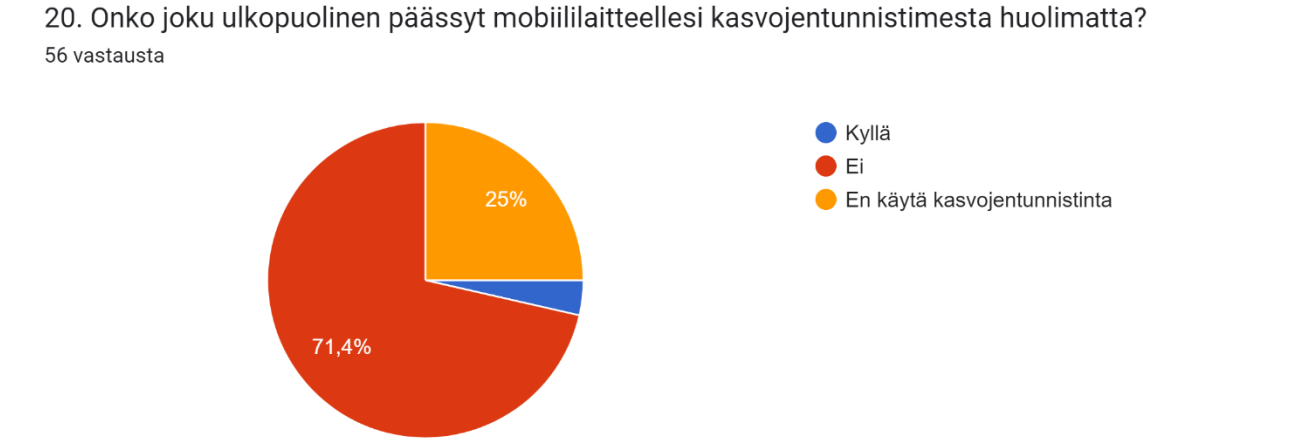
Kuvio 21. Sormenjälkitunnistimen murtaminen

Suurimmat haasteet kasvojentunnistimen kanssa koskivat tunnistuksen epäonnistumista pimeässä ja vastaajilla 53,6 % oli tunnistuksen epäonnistumista tästä syystä. Toiseksi eniten vastattiin, että tunnistus oli epäonnistunut muuten, ilman tarkkaa tietoa miksi (42,9 %). 35,7 % vastasi, että tunnistus oli epäonnistunut silmä- tai aurinkolasien kanssa. 26,8 % vastaajista ei käyttänyt kasvojentunnistusta. Laitteen lukituksen vahingossa avaamisen oli tunnistanut ongelmaksi 19,6 % vastaajista. 16,1 % vastaajista oli epäonnistunut tunnistuksessa liian kirkkaassa. Muu -vaihtoehto kohtaan vastattiin, että tunnistus oli epäonnistunut päähineen kanssa ja isojen kuulokkeiden kanssa. Yksi vastaajista vastasi ongelmatilanteena olleen sen, että hänen sisarensa sai puhelimen auki omilla kasvoillaan. (Kuvio 22.)



Kuvio 22. Kasvojentunnistimen ongelmatilanteita

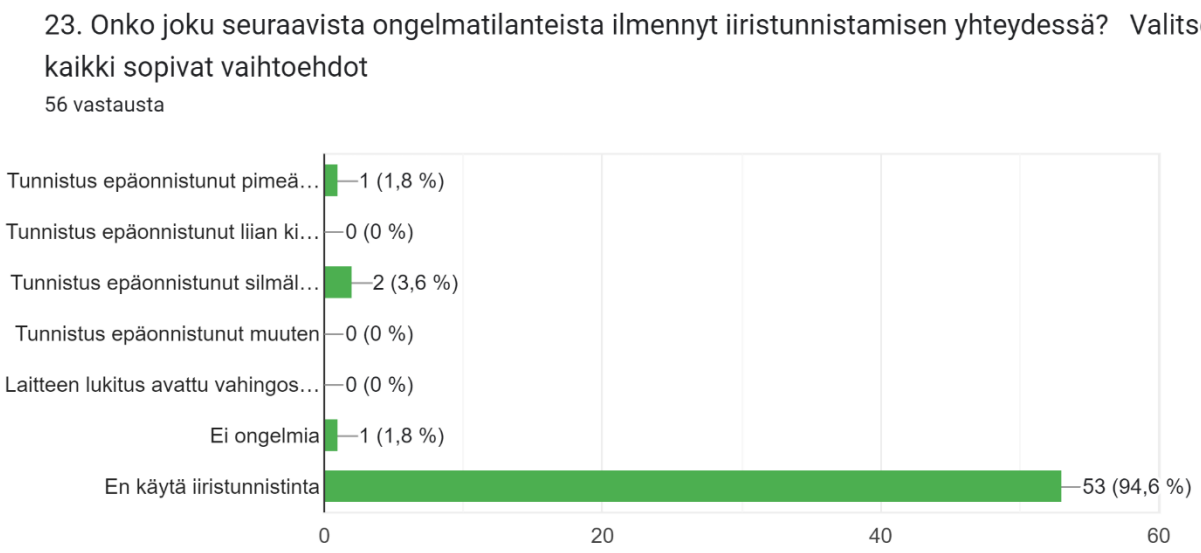
71,4 % vastaajista vastasi, että kukaan ulkopuolinen ei ollut päässyt heidän laitteelleen kasvojentunnistuksen ollessa käytössä. 25 % vastaajista ei käyttänyt kasvojentunnistusta. 3,6 % vastaajista kertoi ulkopuolisen päässeen heidän laitteelleen kasvojentunnistimesta huolimatta. (Kuvio 23.)



Kuvio 23. Kasvojentunnistimen murtaminen

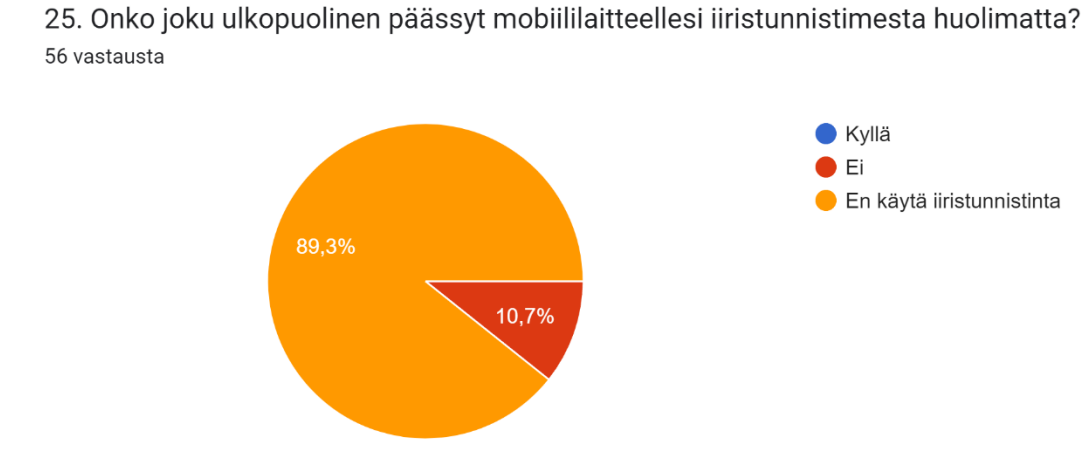
Suurin osa vastaajista ei käyttänyt iiristunnistinta (94,6 %). 3,6 % vastaajista oli kokenut tunnistuksen epäonnistumista silmä- tai aurinkolasien kanssa. 1,8 % vastasivat tunnistuksen

epäonnistuneen pimeässä ja 1,8 % vastaajista ei ollut kohdannut ongelmatilanteita iiristunnistimen kanssa. (Kuvio 24.)



Kuvio 24. Iiristunnistimen ongelmatilanteita

89,3 % vastaajista ei käyttänyt iiristunnistinta. 10,7 % vastasi, että kukaan ulkopuolinen ei ollut päässyt heidän laitteelleen iiristunnistuksen ollessa käytössä. (Kuvio 25.)



Kuvio 25. Iiristunnistimen murtaminen

5 Pohdinta ja johtopäätökset

Tässä viimeisessä luvussa käydään ensiksi läpi tutkimuksen luotettavuutta käsitteiden pätevyys eli validiteetti ja luotettavuus eli reliabiliteetti avulla. Sen jälkeen käydään läpi tutkimuksen tulosten yhteenvetoa sekä tuloksista saadut johtopäätökset. Luvun lopussa käydään läpi kehitysehdotuksia ja opinnäytetyöprosessia kokonaisuudessaan.

5.1 Tutkimuksen tulosten validiteetti ja reliabiliteetti

Validiteetti kuvaa sitä, että tutkimuksen kuuluisi mitata sitä, mitä oli tarkoitus selvittää. Validius tarkoittaa myös systemaattisten virheiden puuttumista. Se on varmistettava etukäteen tarkalla suunnittelulla ja tiedonkeruulla. Kyselylomakkeen kysymysten tulisi mitata oikeita asioita yksiselitteisesti kattaen koko tutkimusongelman. (Heikkilä 2014, 27.)

Reliabiliteetilla taas tarkoitetaan tulosten tarkkuutta eli tutkimuksen tulokset eivät saisi olla sattumanvaraisia. Tämä tarkoittaa sitä, että tutkimus voitaisiin toistaa samanlaisilla tuloksilla, jos se tehtäisiin nyt uudestaan. Luotettavien tulosten ehtona on myös se, että tutkimuksen kohderyhmä ei ole vino eli otos edustaa koko tutkittavaa perusjoukkoa. (Heikkilä 2014, 28.)

Opinnäytetyöni tulosten validiteettia voidaan mielestäni pitää kohtalaisen hyvänä. Kyselylomakkeen kysymykset oli laadittu tarkasti ja kysymykset oli muotoiltu mahdollisimman yksiselitteisiksi ja helposti ymmärrettäviksi. Kaikkiin kysymyksiin oli valmiit vastausvaihtoehdot, millä varmistettiin vastaamisen helppous. Vastaajille annettiin aina myös vastausvaihtoehto, jonka pystyi valitsemaan, jos vastaajilla ei ollut kokemusta tai tietoa jostakin osa-alueesta. Kaiken kaikkiaan tutkimuksessa mitattiin mielestäni juuri sitä, mitä pitikin mitata varsinaisiin tutkimusongelmiin nähden.

Saatujen tulosten perusteella tutkimuksen reliabiliteettia voidaan pitää luotettavana. Toki otoksen osalta täytyy huomioida se, että lähes 80 % vastaajista oli alle 35-vuotiaita, joten vanhempien ihmisten puuttuminen voi vääristää tuloksia. Tutkimus voitaisiin silti mielestäni toistaa nyt ja saada vastaavat tulokset suurella todennäköisyydellä. Lisäksi tutkimuksen toistamisessa pitää ottaa myös huomioon teknologian kova kehitys ja erilaiset laitevalmistajien trendit, joten vastaavan tutkimuksen tulokset tulevat todennäköisesti muuttumaan tulevaisuudessa.

5.2 Tulosten yhteenveto ja johtopäätökset

Tutkimuksen tavoitteena oli vastata tutkimuskysymykseen: *Miten yksityiskäyttäjät kokevat biometriset tunnistusmenetelmät?* Tutkimuskysymykseen haettiin myös vastauksia seuraavien alaongelmien kautta: *Suosivatko yksityiskäyttäjät sormenjälki-, kasvojen- vai iiristunnistinta biometrisistä*

tunnistusmenetelmistä? Mitä haasteita yksityiskäyttäjät ovat kohdanneet biometrisiin tunnistusmenetelmiin liittyen?

Tulosten perusteella tavoitteet saavutettiin, sillä tutkimuskysymykseen ja alaongelmiin saatiin vastaukset. Lisäksi tutkimuksen tavoitteena oli saada vähintään 30 vastaajaa ja lopulta kyselyyn vastasi 56 vastaajaa, joten vastaajamäärässä päästiin reippaasti yli tavoitteen.

Tulosten perusteella biometristen tunnistusmenetelmien käytettävyys koettiin hyvänä. 75 % vastaajista oli useimmiten tyytyväinen käyttämäänsä biometriseen tunnistusmenetelmään. Sormenjälkitunnistimen käytettävyyden koki taas hyväksi 53,6 % vastaajista ja 16,1 % vastaajista koki käytettävyyden erinomaiseksi. Kasvojentunnistimen käytettävyys oli hyvällä tasolla, sillä yli puolet vastaajista koki sen olevan joko hyvä tai erinomainen. Iiristunnistimen käytettävyyteen ei voida todeta juurikaan mitään merkittävää, koska 89,3 % vastaajista ei ollut käyttänyt sitä. Näistä tuloksista voidaan kuitenkin todeta, että biometristen tunnistusmenetelmien nykyinen taso on saavuttanut hyvän käytettävyyden.

Biometrisiä tunnistusmenetelmiä pidettiin yleisesti luotettavina. Vastaajat kokivat sormenjälkitunnistimen olevan tietoturvallisin vaihtoehto, koska selvästi yli puolet vastaajista koki sen tietoturvallisuuden olevan hyvä tai erinomainen. Kasvojentunnistimen osalta sen tietoturvallisuuden koettiin olevan tyydyttävällä tai hyvällä tasolla. Iiristunnistimen osalta ei jälleen kerran voida todeta mitään, koska vastaajat eivät olleet käyttäneet sitä.

Vastaajista vain yhden laitteelle oli päästy luvatta sormenjälkitunnistimesta huolimatta. Kasvojentunnistin oli suojannut kaikkien paitsi kahden vastaajan laitteita luvattomalta käytöltä. Iiristunnistimen osalta ei voida sanoa mitään, koska vastaajat eivät olleet käyttäneet sitä tarpeeksi tulosten saamiseen. Nämä luvut kertovat kuitenkin sen, että biometristen tunnistusmenetelmien tietoturvallisuus laitteiden luvattoman käytön estämisessä on erittäin hyvällä tasolla. Biometrisiin tunnistusmenetelmiin liittyy kuitenkin muitakin tietoturvallisuutta koskevia epäkohtia, kuten biometristen tunnistetietojen säilytyksen tietoturvallisuus. Tämän tutkimuksen osalta tähän ei saatu vastauksia, koska kyselyn tietoturvallisuutta koskevat kysymykset oli tarkoitettu kartoittamaan tietoturvallisuutta mobiililiatteen luvattoman käytön merkityksessä.

Tutkimustuloksista voidaan todeta, että yksityiskuluttajat suosivat biometrisistä tunnistusmenetelmistä eniten sormenjälkitunnistinta sekä kasvojentunnistinta. Vastaajista 50 eli 89,3 % oli käyttänyt sormenjälkitunnistinta. Tämä johtuu luultavasti siitä, että älypuhelimissa ja uusissa kannettavissa tietokoneissa on nykyään oletuksena sormenjälkitunnistin ja siitä on jo muodostunut tietynlainen standardi. Toiseksi suosituin biometrinen tunnistusmenetelmä oli kasvojentunnistin ja 40 vastaajaa

eli 71,4 % käytti sitä. Kasvojentunnistimen suosio on luultavasti kasvanut johtuen Applen siirtymisestä pois sormenjälkitunnistimesta (ks. 2.1.6) ja vastaajista 26 eli 46,4 % käytti Applen iOS käyttöjärjestelmää.

Iiristunnistin ei ollut vastaajien suosiossa ja kyselyyn vastaajista vain kaksi oli käyttänyt iiristunnistinta. Tämä johtunee Samsungin päätöksestä lopettaa iiristunnistimilla valmistettavien laitteiden valmistuksen vuonna 2018 julkaistun Note 9 älypuhelimen jälkeen (Triggs 14.1 2019), eivätkä muut laitevalmistajat ole paikanneet tätä aukkoa markkinoilla.

Vain 4 vastaaja eli 7,1 % ei käyttänyt ollenkaan mitään biometristä tunnistusmenetelmää. Tätä lukua voidaan pitää hieman yllättävän, mutta selvästi biometristen tunnistusmenetelmien yleisyyden ja helppokäyttöisyyden takia suurin osa kuluttajista on siirtynyt niiden käyttöön. Tuloksista kävi myös ilmi, että kuluttajat halusivat jatkaa nykyisten biometristen tunnistusmenetelmien käyttöä. Kiinnostusta iiristunnistinta kohtaan ei ollut kovinkaan paljoa, johtuen sen melko tuntemattomasta maineesta.

Vastaajilla oli oletettavasti hankaluuksia kysymyksissä, jossa kysyttiin tarkemmin kyseisten biometristen tunnistusmenetelmien tyyppiä. Keskivertokuluttaja ei ole teknisesti niin kiinnostunut, että he tietäisivät mikä teknologia on ratkaisujen taustalla.

Biometristen tunnistusmenetelmien kanssa ilmeni paljon haasteita. Sormenjälkitunnistimen kanssa yleisimmät ongelmat liittyivät luonnollisesti sormiin. Useimmiten ongelmat olivat johtuneet märistä, likaisista tai liian kuivista käsistä. Yllättävästi 22 vastaajaa eli 39,3 % oli kokenut ongelmia sormenjälkitunnistimen kanssa pakkasella. Lisäksi yksi vastaajista oli vahingoittanut sormenpäänsä, joten luvussa 2.1.7 käsiteltyä uutta tutkimusta monen sormenjäljen käytöstä, voisi käyttää hyödyksi tämän kaltaisissa tapauksissa.

Kasvojentunnistimen kanssa suurimpina haasteina olivat muun muassa liian pimeät olosuhteet ja tunnistuksen epäonnistuminen silmälasien tai aurinkolasien kanssa. Kasvojentunnistimen tunnistuksen epäonnistumista ei osattu kertoa myöskään kovinkaan tarkasti, koska vastaajista 24 eli 42,9 % ei osannut kertoa tunnistuksen epäonnistumisen syytä. Jälleen kerran iiristunnistimen osalta ei voida vetää mitään muita johtopäätöksiä kuin sen, että kuluttajat eivät käytä sitä.

Luvussa 2.1.4 läpikäydyn ultraääneen perustuvan sormenjälkitunnistimen muodostuminen standardiksi voisi auttaa vähentämään sormenjälkitunnistimen kanssa koettujen haasteiden määrää, sillä ne toimivat paremmin märillä käsillä (Brant 28.6.2017). Myös useamman sormenjäljen

automaattisesti tunnistava lukija voisi vähentää ongelmia tunnistuksessa muun muassa likaisten sormien kanssa (ks. 2.1.7).

Kasvojentunnistimen kanssa koettuja haasteita voi vähentää siirtymällä tavallisesta etukameralla toimivasta tunnistimesta, joko infrapunaan perustuvaan kasvojentunnistimeen, tai 3D-kuvaan perustuvaan kasvojentunnistimeen. Näiden kasvojentunnistintyyppien etuna on niiden parempi toimivuus pimeissä olosuhteissa (Triggs 14.1 2019). (Ks. 2.2.2, 2.2.3).

Verrattuna aikaisempiin tutkimustuloksiin (ks. 2.5), kuten Rauramon (2018, 21, 22) opinnäytetyön tuloksiin, on biometristen tunnistusmenetelmien käyttö kasvanut huomattavasti viiden vuoden aikana. Rauramon 47 vastaajasta vain 7,3 % käytti sormenjälkitunnistinta, ja kasvojentunnistinta vain 0,4 %. Jos näitä lukuja verrataan tutkimukseni tuloksiin, niin nyt 56 vastaajasta 89,3 % käytti sormenjälkitunnistinta ja kasvojentunnistinta käytti 71,4 % vastaajista. Tämä suuri ero tutkimusten välillä voi luultavasti johtua siitä, että mobiililaitteiden biometriset tunnistusmenetelmät ovat viiden vuoden aikana saavuttaneet kuluttajien hyväksynnän, ja laitevalmistajien markkinoille tuomat uudet mobiililaitteet ovat myös kehittyneet paremmalle tasolle käytettävyyden ja toimivuuden osalta.

Rauramon tutkimuksesta kävi ilmi, että biometrisiä tunnistusmenetelmiä kohtaan oli kiinnostusta ja kyselyyn vastaajat toivoivat tulevaisuudessa käytettäviksi tunnistusmenetelmiksi sormenjälkitunnistinta (17,6 %), iiristunnistinta (10,1 %) ja kasvojentunnistinta (8,8 %) (Rauramo 2018, 27). Tutkimuksessani vastaajista 60,7 % halusi käyttää sormenjälkitunnistinta, 60,7 % kasvojentunnistinta ja 16,1 % iiristunnistinta.

Jos tutkimuksestani saatuja tuloksia vertaa vielä Entrust Cybersecurity -instituutin tekemän kyselyn tuloksiin (ks. 2.5), huomataan, että kyselyiden tulokset vastaavat hyvin toisiaan. Suurin osa kuluttajista on käyttänyt biometrisiä tunnistusmenetelmiä säännöllisesti Entrust Cybersecurityn kyselyssä. Lisäksi Entrust Cybersecurityn kyselyn tuloksista on havaittu, että sormenjälkitunnistinta on pidetty hieman luotettavampana kuin kasvojentunnistinta. (Entrust Cybersecurity Institute 2023, 2, 3, 9.) Myös minun tutkimuksessani huomattiin, että biometristen tunnistusmenetelmien käyttö on säännöllinen osa kuluttajien elämää. Vastaavasti tutkimukseni tulosten perusteella sormenjälkitunnistinta pidettiin luotettavampana kuin kasvojentunnistinta.

5.3 Kehittämisehdotukset

Näin jälkeenpäin katsottuna lisäisin kyselyyn kysymyksen koskien sitä, mitä muita tunnistusmenetelmiä yksityiskuluttajat käyttävät biometristen tunnistusmenetelmien lisäksi. Tästä olisi saanut

hyvää vertailukohtaa siihen, kuinka paljon perinteisiä, sekä muita uusia tunnistusmenetelmiä käytetään verrattuna biometrisiin tunnistusmenetelmiin tai samaan aikaan niiden rinnalla.

Lisäksi olisi ollut hyvä lisätä kysymys koskien sitä, millä laitteilla vastaajat käyttivät eniten mitäkin biometristä tunnistusmenetelmää. Olisi ollut myös hyvä miettiä sitä, että kaikkiin kysymyksiin ei olisi ollutkaan pakko vastata. Lisäksi jälkeenpäin miettisin vastausvaihtoehdon ”En käytä biometristä tunnistusmenetelmää” poistamista joistakin mielipiteitä koskevista kysymyksistä. Moneen kysymykseen olisi kuitenkin voinut antaa mielipiteen siitä huolimatta, että ei itse käyttänyt kyseistä biometristä tunnistusmenetelmää. Tämän vastausvaihtoehdon laittaminen helpotti vastaajien ”vastuuta” antaa mielipidettä ja näin mielipiteitä tiettyihin kysymyksiin tuli vähemmän.

5.4 Opinnäytetyöprosessi ja oma oppiminen

Itse opinnäytetyön tekeminen sujui erittäin hyvin, koska aihe opinnäytetyöhön valikoitui jo tutkimusprosessikurssin aikana. Tämän takia olin löytänyt jo hyviä lähteitä ja itse tietopohjaa oli jo kertynyt paljon. Olin aikatauluttanut opinnäytetyöni anteliaalla kädellä ja välillä tuntui, että aikaa oli jopa liikaa. Toki itse kyselyyn ja vastausten purkamiseen meni paljon aikaa ja se oli työläämpää kuin olin alkuun ajatellut.

Myös seminaarista saadusta palautteesta oli paljon hyötyä ja jouduin näin muokkaamaan tiettyjä asioita vielä opinnäytetyön loppupuolella. Opinnäytetyön ohjaajani antoi minulle paljon omaa tilaa opinnäytetyön tekemiseen ja ei juurikaan vaikuttanut kyselyn kysymyksiin tai opinnäytetyön rakenteeseen. Sain kuitenkin tarvittaessa hyvin yhteyttä ohjaajaani, sekä erittäin tärkeää palautetta opinnäytetyöstäni. Lisäksi opinnäytetyön tekemiseen oli saatavilla paljon hyviä ohjeita, jotka auttoivat koko prosessin aikana.

Motivaation ja jaksamisen osalta tuntui, että opinnäytetyön alku- ja keskivaiheessa oli paljon energiaa ja motivaatiota, mutta loppuvaiheilla oli hieman hankaluuksia saada vietyä työ maaliin asti. Kaiken kaikkiaan koko prosessia voidaan pitää onnistuneena tavoitteiden ja aikataulun suhteen. Opinnäytetyötä tehdessäni opin paljon lisää tietoa biometrisitä tunnistusmenetelmistä ja miten tutkimuksia ja pidempiä raportteja tehdään. Tulevaisuudessa minulla on paljon paremmat eväät vastaavien tutkimusten tekemiseen.

Opinnäytetyöni tulokset ovat kuitenkin mielestäni loppujen lopuksi vain viittaa antavia. Siksi olisi todella mielenkiintoista toteuttaa jatkotutkimus paljon suuremmalla skaalalla isolle mobiililaitevalmistajalle tai keskittyä vain mobiililaitteiden biometristen tunnistusmenetelmien haasteisiin tai

tietoturvaan. Toki tämänkin tutkimuksen tuloksia voi käyttää jo nyt hyödyksi, kun lähdetään kehittämään seuraavan sukupolven biometrisiä tunnistusmenetelmiä.

Lähteet

Ajankohtaista. 2023. "Mikä on biometrinen tunnistus". EMCE. Luettavissa: https://ajankohtaista.emce.fi/mik%C3%A4-on-biometrinen-tunnistus. Luettu 31.1.2024.

Android Open Source Project. 2024a. Security features. Luettavissa: https://source.android.com/docs/security/features/biometric. Luettu 26.2.2024.

Android Open Source Project. 2024b. Biometric measurement. Luettavissa: https://source.android.com/docs/security/features/biometric/measure. Luettu 26.2.2024.

Android Open Source Project. 2024c. Fingerprint HAL. Luettavissa: https://source.android.com/docs/security/features/authentication/fingerprint-hal. Luettu 26.2.2024.

Android Open Source Project. 2024e. Face Authentication. Luettavissa: https://source.android.com/docs/security/features/biometric/face-authentication. Luettu 26.2.2024.

Apple. s.a. Face ID:n käyttöönotto iPhonessa. Luettavissa: https://support.apple.com/fi-fi/guide/iphone/iph6d162927a/ios. Luettu: 29.2.2024.

Apple 2023a. Tietoja edistyksellisestä Face ID -tekniikasta. Luettavissa: https://support.apple.com/fi-fi/102381. Luettu 29.2.2024.

Apple 2023c. Tietoja Touch ID:n edistyksellisestä suojausteknologiasta. Luettavissa: https://support.apple.com/fi-fi/105095. Luettu 29.2.2024.

Verkkojulkaisu

Brant, T. 28.6.2017. New Fingerprint Readers Scan Through Water, Glass, Metal. PC Magazine. Luettavissa: https://www.pcmag.com/news/new-fingerprint-readers-scan-through-water-glass-metal. Luettu: 28.4.2024.

Bigelow, S. 2022. Windows 10 (Microsoft Windows 10). TechTarget. Luettavissa: https://www.techtarget.com/searchenterprisedesktop/definition/Windows-10. Luettu: 29.2.2024.

The Britannica Dictionary 2024. Flagship. Luettavissa: https://www.britannica.com/dictionary/flagship. Luettu: 22.2.2024.

Verkkojulkaisu

Dent, S. 17.10 2019. Samsung will fix bug that lets any fingerprint unlock a Galaxy S10. Engadget. Luettavissa: https://www.engadget.com/2019-10-17-samsung-patch-fingerprint-reader.html. Luettu: 10.2.2024.

Verkkojulkaisu

Edwards, B. 13.5.2022. Which iPhones Have Touch ID? How-To Geek. Luettavissa: https://www.howtogeek.com/802122/which-iphones-have-touch-id/. Luettu: 13.3.2024.

Entrust cybersecurity institute 2023. The future of identity report. Luettavissa: https://www.entrust.com/-/media/documentation/reports/csi-future-of-identity-re.pdf?la=en&hash=AC8375292688DC14AB8F82D7A7F42B77. Luettu: 22.2.2024.

Verkkojulkaisu

Feldman, B. 12.7.2017. Replacing Touch ID With Face ID Is a Worse Idea Than You Think. Intelligencer. Luettavissa: https://nymag.com/intelligencer/2017/09/replacing-touch-id-with-face-id-is-worse-than-you-think.html. Luettu: 26.2.2024.

Google. s.a. a. Unlock your Pixel phone with your fingerprint. Luettavissa: https://support.google.com/pixelphone/answer/6285273?hl=en#zippy=%2Con-pixel-and-later-phones-including-fold-follow-these-steps%2Con-pixel-a-g-and-earlier-phones-follow-these-stepsl. Luettu: 29.2.2024.

Google. s.a. b. Unlock your Pixel phone with your face. Luettavissa: https://support.google.com/pixelphone/awer/9517039?hl=en&ref_topic=7083614&sjid=18342539935113598633-EU. Luettu: 29.2.2024.

Google. s.a. c. Fix issues with your fingerprint sensor on your Pixel phone. Luettavissa: https://support.google.com/pixelphone/answer/13537318?hl=en&ref_topic=7083614&sjid=3774772198582384553-EU#zippy=. Luettu: 29.2.2024.

Guo, G., Ray, A., Izydorczak, M., Goldfeder, J., Lipson, H. & Xu, W. 2024. Unveiling intra-person fingerprint similarity via deep contrastive learning. Science Advances,10, 2 s. 1–6. Luettavissa: https://www.science.org/doi/10.1126/sciadv.adi0329. Luettu: 26.2.2024.

Haaga-Helia. "Eettiset periaatteet". Luettavissa: https://student.home.haaga-helia.fi/group/pakki/eettiset-periaatteet. Luettu: 14.2.2024.

Heikkilä, T. 2014, Tilastollinen tutkimus, [9. uudistettu painos] edn, Edita, Helsinki.

Verkkojulkaisu

Hern, A. 23.5.2017. Samsung Galaxy S8 iris scanner fooled by German hackers. The Guardian. Luettavissa: https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security. Luettu: 28.2.2024.

Hristov, V. 16.8.2022. Android has written off Face ID way too soon. Luettavissa: https://www.phonearena.com/news/Android-has-written-off-Face-ID-way-too-soon_id141933. Luettu: 26.2.2024.

Ivanova, B. 3.11.2006. fingerprints. Luettavissa: https://www.flickr.com/photos/36736101@N00/232125866. Luettu: 3.5.2024.

Jain, A., Ross, A., & Prabhakar, S. 2004. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20, 1. Luettavissa: https://ieeexplore.ieee.org/document/1262027. Luettu: 7.2.2024.

Jain, A., Klare, B., & Park, U. 2012. Face Matching and Retrieval in Forensics Applications. IEEE MultiMedia. 19. 20. 10.1109/MMUL.2012.4. Luettavissa: https://www.researchgate.net/publication/220634629_Face_Matching_and_Retrieval_in_Forensics_Applications. Luettu: 29.2.2024.

Kodituwakku, S. 2015. BIOMETRIC AUTHENTICATION: A REVIEW. International Journal of Trend in Research and Development. 2. s. 113–123. Luettavissa: https://www.researchgate.net/publication/281257836_BIOMETRIC_AUTHENTICATION_A_REVIEW. Luettu: 7.2.2024.

Microsoft. 11.5.2020. Windows Hello. Luettavissa https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello. Luettu 4.2.2024.

Microsoft. 15.7.2021. Windows Hello face authentication. Luettavissa: https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-face-authentication. Luettu 9.2.2024.

Moorthy S, G., Raaj S, K., Akshayaa, S. & Manoj, B. 2023. The Technology Behind Face Unlocking in Smartphones. International Journal of Research Publication and Reviews, 4, 4, s. 2072. Luettavissa: https://ijrpr.com/uploads/V4ISSUE4/IJRPR11630.pdf. Luettu: 26.2.2024.

Mäki, R. 2020. Mobiililaitteiden sormenjälkitunnistaminen. Alempi AMK-opinnäytetyö. Haaga-Helia ammattikorkeakoulu, Tietojenkäsittelyn koulutusohjelma. Luettavissa: https://urn.fi/URN:NBN:fi:amk-2020060115847. Luettu: 11.2.2024.

Rauramo, R. 2018. Tunnistautumismenetelmät yksityiskäyttäjän näkökulmasta. Alempi AMK-opinnäytetyö. Haaga-Helia ammattikorkeakoulu, Tietojenkäsittelyn koulutusohjelma. Luettavissa: https://urn.fi/URN:NBN:fi:amk-2018111116951. Luettu: 11.2.2024.

Samsung. 4.8.2016. Samsung Newsroom. [In-Depth Look] Keeping an Eye on Security: The Iris Scanner of the Galaxy Note7. Luettavissa: https://news.samsung.com/global/in-depth-look-keeping-an-eye-on-security-the-iris-scanner-of-the-galaxy-note7. Luettu: 29.2.2024.

Statcounter 2023. Mobile Operating System Market Share Worldwide. Luettavissa: https://gs.statcounter.com/os-market-share/mobile/worldwide. Luettu: 4.2.2024.

Verkkojulkaisu

Sweeney, E. 7.7.2024. iOS Explained: Apple's operating system version history, features, and iPhone capabilities. Business Insider. Luettavissa: https://www.businessinsider.com/apple-ios?r=US&IR=T. Luettu: 29.2.2024.

TechTerms. 2023a. "Iris Recognition". TechTerms. Luettavissa: https://techterms.com/definition/irisrecognition. Luettu 3.2.2024.

TechTerms. 2023b. "Facial Recognition". TechTerms. Luettavissa: https://techterms.com/definition/facialrecognition. Luettu 4.2.2024.

TechTerms. 2023c. "PIN (Personal Identification Number)". TechTerms. Luettavissa: https://techterms.com/definition/pin. Luettu 4.2.2024.

TechTerms. 2023d. "Password". TechTerms. Luettavissa: https://techterms.com/definition/password. Luettu 4.2.2024.

TechTerms. 2023e. "Fingerprint Scanner". TechTerms. Luettavissa: https://techterms.com/definition/fingerprint_scanner. Luettu 4.2.2024.

TENK. 2012. "HTK-ohje: Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen". Luettavissa: https://tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf. Luettu: 4.2.2024.

Thomas, G 1.10.2021. Introducing Qualcomm 3D Sonic Sensor Gen 2. OnQ Blog. Luettavissa: https://www.qualcomm.com/news/onq/2021/01/introducing-qualcomm-3d-sonic-sensor-gen-2. Luettu 9.2.2024.

Tietotekniikan termitalkoot, 2005. Sanastokeskus Ry. Luettavissa: https://sanastokeskus.fi/tsk/fi/termitalkoot/haku-266.html. Luettu: 5.2.2024.

Verkkojulkaisu

Triggs, R. 14.1 2019. Facial recognition technology explained. Android Authority. Luettavissa: https://www.androidauthority.com/facial-recognition-technology-explained-800421/. Luettu: 10.2.2024.

Triggs, R. 25.3 2023. How fingerprint scanners work: Optical, capacitive, and ultrasonic explained. Android Authority. Luettavissa: https://www.androidauthority.com/how-fingerprint-scanners-work-670934/. Luettu: 10.2.2024.

Wang, C, Wang, Y, Chen, Y, Liu, H, Liu, J 2020. User authentication on mobile devices: Approaches, threats and trends, Computer Networks, (2020), 107118, 170, 1. Luettavissa: https://www.sciencedirect.com/science/article/abs/pii/S1389128618312799. Luettu 8.2.2024.

Wankhede, C. 16.8.2022. Facial recognition on smartphones: Is it secure and should you use it? Android Authority. Luettavissa: https://www.androidauthority.com/face-unlock-smartphones-3043993/. Luettu 10.2.2024.

Liitteet

Liite 1. Kyselylomake

Mobiililaitteiden biometriset tunnistusmenetelmät:

Tämä kysely on osa opinnäytetyötä "**Mobiililaitteiden biometriset tunnistusmenetelmät: Ratkaisut ja haasteet yksityiskäyttäjän näkökulmasta**" ja sen tarkoituksena on kartoittaa, miten yksityiskäyttäjät kokevat mobiililaitteiden eri biometriset tunnistusmenetelmät, mitkä menetelmät ovat suosioissa ja mitä haasteita niiden käytössä esiintyy. Tutkimusaineisto ja tulokset käsitellään luottamuksellisesti henkilötietolain edellyttämällä tavalla. Lopulliset tutkimustulokset raportoidaan niin, että vastauksia ei voida yhdistää yksittäisiin vastaajiin.

Tutkimukseen vastaaminen vie noin 5–10 minuuttia.

Vastausaikaa on 24.3.2024 asti.

**** merkittyihin kysymyksiin pakko vastata.***

Olmo Kosunen
Tietojenkäsittelyn koulutusohjelma
Haaga-Helia ammattikorkeakoulu

* Pakollinen kysymys

Taustatiedot

1. **1. Ikäryhmä** *

Merkitse vain yksi soikio.

- ◯ 15-24
- ◯ 25-34
- ◯ 35-44
- ◯ 45-54
- ◯ 55-64
- ◯ 65+

2. **2. Tietotekniset taidot** *

Merkitse vain yksi soikio.

- ◯ Erinomaiset
- ◯ Hyvät
- ◯ Kohtalaiset
- ◯ Huonot
- ◯ Erittäin huonot

3. **3. Mobiililaitteeni/kannettavan tietokoneeni käyttöjärjestelmä** *

Valitse kaikki sopivat vaihtoehdot

Valitse kaikki sopivat vaihtoehdot.

- ☐ Android (Google)
- ☐ iOS (Apple)
- ☐ Windows (Microsoft)
- ☐ MacOS (Apple)
- ☐ Muu: _____

Kysymykset

Yleinen kartoitus

4. **4. Mitä seuraavista biometrisistä tunnistusmenetelmistä olet käyttänyt mobiililaitteessasi?** *

Valitse kaikki sopivat vaihtoehdot

Valitse kaikki sopivat vaihtoehdot.

- [ ] Sormenjälkitunnistin
- [ ] Kasvojentunnistin
- [ ] Iiristunnistin
- [ ] En käytä biometristä tunnistusmenetelmää
- [ ] Muu: _____

5. **5. Oletko ollut tyytyväinen käyttämääsi biometriseen tunnistusmenetelmään?** *

Merkitse vain yksi soikio.

- ◯ Aina
- ◯ Useimmiten
- ◯ Välillä
- ◯ Harvoin
- ◯ En koskaan
- ◯ En käytä biometristä tunnistusmenetelmää

6. **6. Mitä biometristä tunnistusmenetelmää haluaisit käyttää mobiililaitteessasi?** *

Valitse kaikki sopivat vaihtoehdot

Valitse kaikki sopivat vaihtoehdot.

- [ ] Sormenjälkitunnistin
- [ ] Kasvojentunnistin
- [ ] Iiristunnistin
- [ ] En halua käyttää biometristä tunnistusmenetelmää
- [ ] Muu: _____

7. **7. Minkä mobiililaitteiden biometrisen tunnistusmenetelmän toivoisit kehittyvän tulevaisuudessa?** *

Valitse kaikki sopivat vaihtoehdot

Valitse kaikki sopivat vaihtoehdot.

- [ ] Sormenjälkitunnistin
- [ ] Kasvojentunnistin
- [ ] Iiristunnistin
- [ ] Ei kehittämisen tarvetta
- [ ] En osaa sanoa

Sormenjälkitunnistin

Seuraavat kysymykset koskevat sormenjälkitunnistinta.

8. **8. Miten koet sormenjälkitunnistimen käytettävyyden?** *

Merkitse vain yksi soikio.

- Erinomainen
- Hyvä
- Tyydyttävä
- Huono
- Erittäin huono
- En osaa sanoa
- En käytä sormenjälkitunnistinta

9. **9. Miten koet sormenjälkitunnistimen tietoturvallisuuden?** *

Merkitse vain yksi soikio.

- Erinomainen
- Hyvä
- Tyydyttävä
- Huono
- Erittäin huono
- En osaa sanoa
- En käytä sormenjälkitunnistinta

10. **10. Millainen sormenjälkitunnistin mobiililaitteessasi on?** *

Merkitse vain yksi soikio.

- ◯ Optinen sormenjälkitunnistin
- ◯ Kapasitiivinen sormenjälkitunnistin
- ◯ Optiskapasitiivinen sormenjälkitunnistin
- ◯ Ultraääneen perustuva sormenjälkitunnistin
- ◯ En osaa sanoa
- ◯ Ei sormenjälkitunnistinta

11. **11. Kuinka monta sormenjälkeä olet lisännyt laitteellesi?** *

Merkitse vain yksi soikio.

- ◯ 0
- ◯ 1-2
- ◯ 3-5

12. **12. Missä yhteydessä olet käyttänyt sormenjälkitunnistusta?** *

Valitse kaikki sopivat vaihtoehdot

Valitse kaikki sopivat vaihtoehdot.

- ☐ Mobiililaitteen lukituksen avaaminen
- ☐ Verkkopankkiin tunnistautuminen
- ☐ Maksutapahtuman vahvistaminen
- ☐ En käytä sormenjälkitunnistinta
- ☐ Muu: _____

13. **13. Onko joku seuraavista ongelmatilanteista ilmennyt sormenjälkitunnistamisen yhteydessä?** *

Valitse kaikki sopivat vaihtoehdot

Valitse kaikki sopivat vaihtoehdot.

- [ ] Tunnistus epäonnistunut märillä käsillä
- [ ] Tunnistus epäonnistunut liian kuvilla käsillä
- [ ] Tunnistus epäonnistunut likaisilla käsillä
- [ ] Tunnistus epäonnistunut pakkasella
- [ ] Tunnistus epäonnistunut liian valoisassa
- [ ] Tunnistus epäonnistunut muuten
- [ ] Laitteen lukitus avattu vahingossa
- [ ] Ei ongelmatilanteita
- [ ] En käytä sormenjälkitunnistinta
- [ ] Muu: _____

14. **14. Onko joku ulkopuolinen päässyt mobiililaitteellesi sormenjälkitunnistimesta huolimatta?** *

Merkitse vain yksi soikio.

- ◯ Kyllä
- ◯ Ei
- ◯ En käytä sormenjälkitunnistinta

Kasvojentunnistin

Seuraavat kysymykset koskevat kasvojentunnistinta

15. **15. Miten koet kasvojentunnistimen käytettävyyden?** *

Merkitse vain yksi soikio.

- Erinomainen
- Hyvä
- Tyydyttävä
- Huono
- Erittäin huono
- En osaa sanoa
- En käytä kasvojentunnistinta

16. **16. Miten koet kasvojentunnistimen tietoturvallisuuden?** *

Merkitse vain yksi soikio.

- Erinomainen
- Hyvä
- Tyydyttävä
- Huono
- Erittäin huono
- En osaa sanoa
- En käytä kasvojentunnistinta

17. **17. Millainen kasvojentunnistin mobiililaitteessasi on?** *

Merkitse vain yksi soikio.

- Pelkän etukameran ottamaan kuvaan perustuva kasvojentunnistin
- Infrapunaan perustuva kasvojentunnistin
- 3D-kuvaan perustuva kasvojentunnistin
- En osaa sanoa
- Ei kasvojentunnistinta

18. **18. Onko joku seuraavista ongelmatilanteista ilmennyt kasvojentunnistamisen yhteydessä?** *

Valitse kaikki sopivat vaihtoehdot

Valitse kaikki sopivat vaihtoehdot.

- [ ] Tunnistus epäonnistunut pimeässä
- [ ] Tunnistus epäonnistunut liian kirkkaassa
- [ ] Tunnistus epäonnistunut silmälasien/aurinkolasien kanssa
- [ ] Tunnistus epäonnistunut muuten
- [ ] Laitteen lukitus avattu vahingossa
- [ ] Ei ongelmia
- [ ] En käytä kasvojentunnistinta
- [ ] Muu: _____

19. **19. Missä yhteydessä olet käyttänyt kasvojentunnistusta?** *

Valitse kaikki sopivat vaihtoehdot

Valitse kaikki sopivat vaihtoehdot.

- [ ] Mobiililaitteen lukituksen avaaminen
- [ ] Verkkopankkiin tunnistautuminen
- [ ] Maksutapahtuman vahvistaminen
- [ ] En käytä kasvojentunnistinta
- [ ] Muu: _____

20. **20. Onko joku ulkopuolinen päässyt mobiililaitteellesi kasvojentunnistimesta huolimatta?** *

Merkitse vain yksi soikio.

- ◯ Kyllä
- ◯ Ei
- ◯ En käytä kasvojentunnistinta

Iiristunnistin

Seuraavat kysymykset koskevat iiristunnistinta

21. **21. Miten koet iiristunnistimen käytettävyyden?** *

Merkitse vain yksi soikio.

- ◯ Erinomainen
- ◯ Hyvä
- ◯ Tyydyttävä
- ◯ Huono
- ◯ Erittäin huono
- ◯ En osaa sanoa
- ◯ En käytä iiristunnistinta

22. **22. Miten koet iiristunnistimen tietoturvallisuuden?** *

Merkitse vain yksi soikio.

- ◯ Erinomainen
- ◯ Hyvä
- ◯ Tyydyttävä
- ◯ Huono
- ◯ Erittäin huono
- ◯ En osaa sanoa
- ◯ En käytä iiristunnistinta

23. **23. Onko joku seuraavista ongelmatilanteista ilmennyt iiristunnistamisen yhteydessä?** *

Valitse kaikki sopivat vaihtoehdot

Valitse kaikki sopivat vaihtoehdot.

- [ ] Tunnistus epäonnistunut pimeässä
- [ ] Tunnistus epäonnistunut liian kirkkaassa
- [ ] Tunnistus epäonnistunut silmälasien/aurinkolasien kanssa
- [ ] Tunnistus epäonnistunut muuten
- [ ] Laitteen lukitus avattu vahingossa
- [ ] Ei ongelmia
- [ ] En käytä iiristunnistinta
- [ ] Muu: _____

24. **24. Missä yhteydessä olet käyttänyt iiristunnistusta?** *

Valitse kaikki sopivat vaihtoehdot

Valitse kaikki sopivat vaihtoehdot.

- [ ] Mobiililaitteen lukituksen avaaminen
- [ ] Verkkopankkiin tunnistautuminen
- [ ] Maksutapahtuman vahvistaminen
- [ ] En käytä iiriistunnistinta
- [ ] Muu: _____

25. **25. Onko joku ulkopuolinen päässyt mobiililaitteellesi iiristunnistimesta huolimatta?** *

Merkitse vain yksi soikio.

- ◯ Kyllä
- ◯ Ei
- ◯ En käytä iiristunnistinta

Kiitos arvokkaista vastauksista!

-Olmo Kosunen, tietojenkäsittelyn opiskelija