Mobiilivarmenteen tietoturva vahvassa tunnistautumisessa

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tietotekniikka
Maaliskuu 2026
Juho Kauti

TURUN YLIOPISTO
Tietotekniikan laitos

Juho Kauti: Mobiilivarmenteen tietoturva vahvassa tunnistautumisessa

TkK-tutkielma, 25 s.
Tietotekniikka
Maaliskuu 2026

Nykyaikaisessa yhteiskunnassa kaikki kriittiset palvelut toimivat digitaalisessa ympäristössä. Tällöin ne ovat saavutettavissa nopeasti ja silloin, kun ihmiselle sopii. Kuluttaminen, terveydenhuolto, työpaikkojen haku, opintoasiat ja kaikki muukin tapahtuvat lisääntyvissä määrin digitaalisessa maailmassa. Tämä on johtanut tilanteeseen, jossa tarvitaan luotettavia keinoja tunnistaa henkilö digitaalisessa ympäristössä. Tähän tarkoitukseen on luotu järjestelmiä, jotka perustuvat ihmisten yksityisiin resursseihin. Nämä järjestelmät auttavat rajoittamaan arkaluontoisten tietojen näkemistä siten, että tietojen saatavuus ei hankaloidu merkittävästi. Suomessa tähän on kehitetty monia vaihtoehtoja, kuten esimerkiksi mobiilivarmenne.
Tämän työn tarkoituksena oli perehtyä mobiilivarmenteen tekniikkaan ja sen tietoturvan todelliseen tasoon. Lisäksi tarkasteltiin sitä, millainen osuus käyttäjän tiedoilla ja taidoilla voi olla tietoturvan ylläpidossa. Mobiilivarmennetta tarkasteltiin tutkimalla esimerkiksi siihen liittyvien protokollien teknisiä dokumentteja sekä perehtymällä kryptografisiin menetelmiin. Tutkimusmenetelmiin palataan tarkemmin johdannon Menetelmät-osiossa.
Tutkimuksessa mobiilivarmenne osoittautui tekniikaltaan vahvaksi, erityisesti sen toteutuksessa käytettävien kryptografisten menetelmien vahvuuden ansiosta. Jatkuvasti kehittyvän tekniikan takia nyt vallitsevaan hyvään tilanteeseen ei saada kuitenkaan tyytyä. Tämän tiedostaminen on erityisen tärkeää siinä tapauksessa, jos nyt kehitteillä olevat kvanttitietokoneet lyövät läpi, sillä niiden laskentateholla nykyiset algoritmit ovat murrettavissa.

Asiasanat: mobiilivarmenne, tietoturva, kryptografia, kvanttitietokoneet

Sisällys

1 Johdanto

Ihmiskunnan historiassa ensimmäiset nykyaikaisiin tietokoneisiin etäisesti verrattavat koneet kehitettiin 1940-luvulla toisen maailmansodan aikana. Ne olivat nimeltään ENIAC sekä Colossus. ENIAC kehitettiin Yhdysvaltain armeijan käyttöön, ja sen tehtävä oli avustaa ohjusten maalitaulujen laskemisessa [1]. Colossus kehitettiin Isossa-Britanniassa saksalaisten salakirjoituskoodin (Lorenz-salaus) murtamiseen [2]. 1960-luvulla Yhdysvalloissa heräsi tarve kehittää kommunikointitekniikoita. Erityisesti yhdysvaltalaiset yliopistot sekä korkean puolustusteknologian toimijat haluttiin yhdistää. Tästä tarpeesta syntyi idea rakentaa ARPANET (Advanced Research Projects Agency Network) [3].

1970 -luvulla ARPANETin suosio kasvoi merkittävästi, erityisesti sen yhteyteen kehitetyn sähköpostiohjelman ansiosta. Suosion kasvaessa heräsi erityisesti Yhdysvalloissa huoli siitä, että hallituksen ja armeijan salaiset tiedot, jotka myös liikkuivat ARPANETissä, voisivat vuotaa muiden tietoon. Tästä syystä ARPANET jaettiin kahdeksi verkoksi, joista toinen, MILNET, oli tarkoitettu hallitukselle ja armeijalle, ja toisesta kehittyi Internet [3].

Internetin laajamittaiseen käyttöönottoon tarvittiin kuitenkin vielä uutta teknologiaa. Alusta lähtien ideana oli, että Internet rakentuu useista pienemmistä verkoista. ARPANETissä datan siirtoa varten oli kehitetty NCP (Network Control Protocol). Se pystyi kuitenkin operoimaan vain yhtä verkkoa, jonka laitteisto oli kontrolloitavissa. Niinpä vuodesta 1972 ARPANETin parissa työskennellyt Robert E.

Kahn päätti kehittää yhdessä Vinton G. Cerfin kanssa TCP-protokollan (Transmission Control Protocol) [4]. Näin luotiin perusta pakettikytkentäiselle verkolle, jossa tieto liikkuu datagrammeina eli niin sanottuina IP-paketteina.

Vähitellen TCP-protokolla jakautui kahdeksi erilliseksi protokollaksi, koska sen uudelleenlähetysominaisuus koettiin joissain yhteyksissä jopa haitalliseksi. TCP-protokollan tehtäväksi määritettiin luoda luotettava yhteydellinen tiedonsiirtoprotokolla, jota käytetään segmenttien lähettämiseen. TCP hoitaa myös segmenttien uudelleenlähetyksen [4]. IP-protokollan (Internet Protocol) tehtäväksi määritettiin TCP-segmenttien paketoiminen datagrammeiksi, datagrammien osoitteistaminen sekä lähettäminen ja reititys [5]. Merkittävä osa nykyaikaisesta verkkoteknologiasta rakentuu TCP/IP:lle [3] [6].

Internetin käyttö yleistyi voimakkaasti 1990-luvulla. Tähän suuri vaikutus oli *World Wide Webillä (WWW)* [7], joka on Tim Berners-Leen Cernissä vuonna 1989 kehittämä hypertekstin siirtojärjestelmä. Sen ideana on yhdistää dokumentteja toisiinsa hyperlinkkien välityksellä [8]. Näin navigointi dokumenttien välillä onnistuu helpommin.

Toinen 1990-luvulla Internetin levinneisyyttä edistänyt asia oli verkkoselainten ilmestyminen markkinoille [9]. Ensimmäisiä selaimia olivat muun muassa NCSA Mosaic sekä Netscape Navigator. Vähitellen kaiken datan siirtyessä verkkoon, kasvoi myös tarve luotettaville tunnistautumiskeinoille. Nykyään vahva sähköinen tunnistautuminen on käytännössä välttämätön edellytys esimerkiksi pankkiasioiden hoitamisessa ja viranomaisten kanssa asioimisessa.

1.1 Työn tavoite

Tämän työn tarkoituksena on tutkia mobiilivarmenteen luotettavuutta vahvan sähköisen tunnistautumisen välineenä. Työssä tutkitaan sitä, kuinka vaikeaa mobiilivarmenteen tekniikka on murtaa ja kuinka paljon se kestää käyttäjän virheitä.

Työn on tarkoitus perehdyttää siihen, miten mobiilivarmenne teknisesti toimii ja mitä protokollia sen taustalla on. Lisäksi perehdytään teorioihin, jotka toimivat näiden protokollien perustana.

Tutkimus aloitetaan tutustumalla siihen, mitä tunnistautuminen ja sähköinen tunnistautuminen käsitteinä tarkoittavat sekä miten ne on toteutettu aikana ennen mobiilivarmennetta. Näitä asioita käsitellään luvussa 2. Luvussa 3 käsitellään mobiilivarmenteen tekniikkaa ja sitä, kuinka murtovarma se on. Luvussa 4 tehdään yhteenveto tutkimuksen tuloksista ja pohditaan, mitä mahdollisia kehityskohteita mobiilivarmenteella voisi tulevaisuudessa olla. Työn tutkimuskysymykset ovat:

TK1:Miten SIM-kortille tallennettu mobiilivarmenne teknisesti toteutetaan ja miten se mahdollistaa vahvan tunnistautumisen?

TK2:Mitkä ovat mobiilivarmenteen keskeiset uhat sekä teknisesti että käyttäjän näkökulmasta?

1.2 Tiedonhaku

Tiedonhaku toteutettiin useassa vaiheessa kirjoitustyön aikana. Lähteitä etsittiin työn edistymisen myötä. Aluksi tiedonhaussa keskityttiin hakemaan tietoa muodostamalla hakulauseita aiheeseen liittyvistä keskeisistä käsitteistä. Tälläisiä käsitteitä olivat esimerkiksi julkisen avaimen infrastruktuuri (eng. Public Key Infrastructure, PKI), kryptografia (cryptography), uhat (threats), tietojen kalastelu (phishing) sekä kvanttilaskenta (quantum computing). Lisäksi käytettiin näihin käsitteisiin liittyvien asioiden nimiä, esimerkiksi kryptografiasta hakiessa käytettiin algoritmien nimiä kuten SHA-256. Loppuvaiheessa työssä siirryttiin käyttämään hakuja, joissa ei ollut varsinaista hakulauseketta (lause ei sisältänyt esimerkiksi operaattoreita), kuten esimerkiksi "rfc 791 internet protocol Jon Postel".

Tietokantoina käytettiin pääasiassa Volteria sekä IEEE Xplorea. Tuloksena saatuja artikkeleita seulottiin tutkimalla ensiksi sitä, ovatko ne työhön sopivia lähtei-

tä ja toisena painotettiin vertaisarviointia. Joitakin lähteitä on haettu tietokantojen ulkopuolelta, mutta ne ovat luotettavista lähteistä (Finlex, Suomi.fi), ja niiden ajantasaisuus on voitu varmistaa. Lähteenä on myös käytetty vuodelta 2009 olevaa opinnäytetyötä. Se valikoitui mukaan, koska tarkoituksena oli kertoa aiheen historiasta. Lisäksi valitussa työssä oli useita luotettuja ja vertaisarvioituja lähteitä pohjana.

Tekoälyä käytettiin tuottamaan hakulauseke-ehdotuksia, mutta niitä ei lopulta työssä hyödynnetty. Lisäksi tekoälyä pyydettiin tekemään tiivistelmät joistakin löydetyistä artikkeleista, jolloin saatiin nopea käsitys siitä, ovatko artikkelit tutkielman aiheeseen sopivia. Artikkelien sisältö on kuitenkin tarkastettu, eikä tekoälyä pidetty missään kohtaa luotettavana tiedonlähteenä. Tekoälyä käytettiin antamaan nopeaa palautetta työstä aina silloin, kun se oli tarpeellista. Lisäksi työtä läpikäydessä tekoälyä käytettiin antamaan mielipide väitteiden oikeellisuudesta suhteessa lähteisiin, mutta tässäkään kohdassa tekoälyä ei pidetty luotettavana lähteenä, vaan lähteiden teksti tarkistettiin kirjoittajan toimesta ennen kuin mahdollisia korjauksia tehtiin.

Yhteenveto

Tässä kappaleessa tutustuttiin TCP/IP -protokollapinon historiaan, Internetin syntymiseen ja kasvuun sekä palveluiden digitalisoitumiseen. Tästä päästiin siihen, miksi vahvaa sähköistä tunnistautumista tarvitaan nykyään. Tämän jälkeen esiteltiin tutkielman aihe, näkökulma sekä tutkimuskysymykset. Lisäksi käytiin läpi tiedonhakuprosessi, tekoälyn rooli ja arvioitiin lähteiden luotettavuutta.

2 Vahva sähköinen tunnistautuminen

Tunnistautuminen käsitteenä tarkoittaa henkilön tunnistamista luotettavasti käyttäen perinteisiä, lain sallimia keinoja. Tällaisia keinoja ovat esimerkiksi henkilön passin, henkilökortin tai henkilötunnuksen tarkistaminen. Ideana on siis käyttää tunnistukseen jotain sellaista resurssia, jonka voidaan perustellusti olettaa olevan vain tämän kyseisen henkilön hallussa.

Sähköinen tunnistautuminen käsitteenä tarkoittaa samaa kuin edellä mainittu *tunnistautuminen*, mutta se tehdään sähköisissä asiointiympäristöissä. Vahvassa sähköisessä tunnistautumisessa henkilökohtaisina todentamistekijöinä toimivat esimerkiksi pankkitunnusten tai mobiilivarmenteen PIN-koodit [10]. Vahva tunnistautuminen on käytännössä aina kaksi- tai useampivaiheinen prosessi. Esimerkiksi pankkitunnuksilla annetaan ensin käyttäjätunnus tunnistautumissivulle, ja sen jälkeen pankin omassa ID-sovelluksessa tunnistustapahtuma hyväksytään ja syötetään PIN-koodi. Kun tunnukset annetaan, järjestelmä tunnistaa luotettavasti, kuka tämä henkilö on, ja - olettaen, että tunnukset ovat oikein - näyttää seuraavaksi tiedot, jotka vain tämä kyseinen henkilö saa nähdä [10]. Poikkeuksena tästä ovat eri ammatit ja niitä suorittavien henkilöiden oikeus nähdä esimerkiksi potilastietoja, mutta niitä ei tässä tutkimuksessa käsitellä.

Laki määrittää vahvalle tunnistautumiselle erittäin tiukat ehdot. Tunnistusvä-

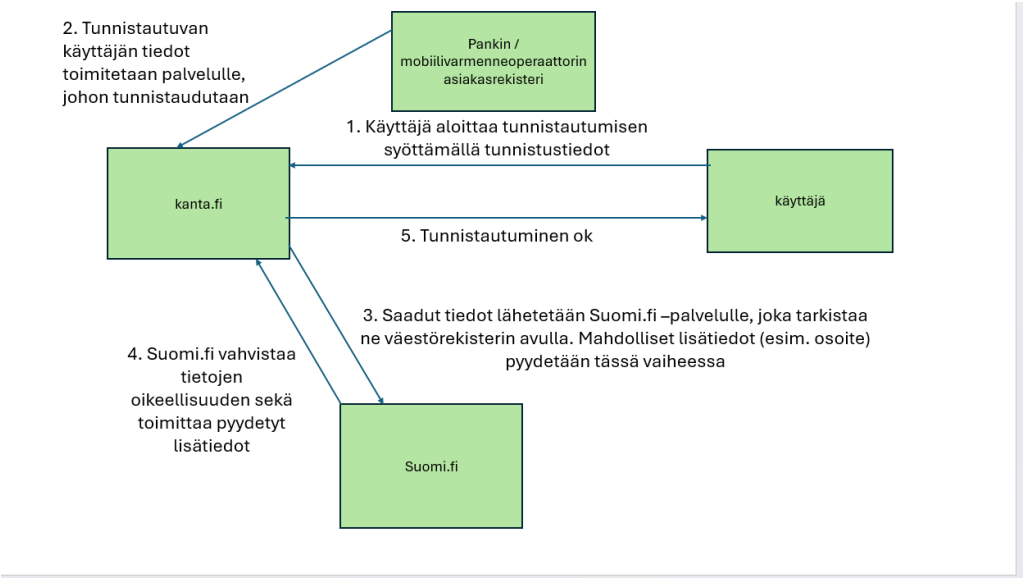
lineen haltija on voitava tunnistaa yksiselitteisesti niin, että EU-komission tasolla asiasta annetut vaatimukset täyttyvät. Lisäksi on saavutettava riittävä varmuus siitä, että ainoastaan tunnistusvälineen haltija voi käyttää tunnistusmenetelmää [11].

Tunnistautumisessa käytettävät välineet ovat myös tarkasti Liikenne- ja viestintävirasto Traficomin sekä lain määrittämiä. Niiden on sisällettävä tietyt tiedot (esimerkiksi varmenteen yksilöivä tunnus ja varmenteen haltijan yksilöivä tunnus), oltava voimassa sekä hyväksytty. Traficom jaottelee tunnistusvälineet korkean tason (henkilökortti, sotealan toimikortti, organisaatiokortit) ja korotetun tason tunnistusvälineisiin (pankkitunnukset, hightrust.id, mobiilivarmenne) [11] [12]. Mobiilivarmenne ei ole keksintönä täysin uusi, vaan monia siinä olevia ratkaisuja, kuten esimerkiksi julkisen avaimen infrastruktuuria (jäljemäpänä PKI) on käytetty jo ennen sitä. Yleisimpiä Suomessa käytettyjä protokollia vahvaan tunnistautumiseen 2000-luvulla olivat: TUPAS-palvelu (pankit), Katso-tunniste (Kela ja Verohallinto) sekä sähköinen henkilökortti (Väestörekisterikeskus) [13].

2.1 SIM-pohjainen tunnistautuminen

SIM-pohjaisessa tunnistautumisessa käyttäjä autentikoidaan (tunnistetaan) kryptografisten avainten ja hänen itse luomansa PIN-koodin avulla. Menetelmässä yksityinen avain tallennetaan SIM-kortille. Avainten luojina toimiviin algoritmeihin palataan tarkemmin seuraavassa luvussa.

Suomessa on kehitetty tunnistautumisen helpottamiseksi Suomi.fi -palvelu. Se voidaan liittää moniin digitaalisiin palveluihin. Palvelu, johon yritetään tunnistautua, saa tunnistuksen yhteydessä käyttäjän tiedot esimerkiksi tunnistusvälinettä tarjoavan palvelun asiakasrekisteristä, ja pyytää Suomi.fi:tä vertaamaan niitä väestötietojärjestelmässä oleviin tietoihin. Jos palvelu tarvitsee lisätietoja käyttäjästä, Suomi.fi hakee pyydetyt lisätiedot väestötietojärjestelmästä ja välittää ne eteenpäin [12]. Suomi.fi:n rooli tunnistautumisessa havainnollistetaan kuvassa 2.1.



Kuva 2.1: Suomi.fi-palvelun rooli vahvassa sähköisessä tunnistautumisessa, esimerkkinä kirjautuminen Kanta.fi-palveluun.

2.2 eIDAS

Sähköinen tunnistautuminen on ottanut kehitysaskelia myös maailmanlaajuisesti. Esimerkiksi Euroopan unioni on säätänyt sähköisestä tunnistautumisesta eIDAS -asetuksen, jonka myötä EU-valtioiden välinen sähköinen tunnistautuminen on helpottunut merkittävästi. eIDAS määrittelee neljä erilaista sähköisen allekirjoituksen tyyppiä, joita ovat: *sähköinen allekirjoitus, eng. Electronic signature*, *kehittynyt sähköinen allekirjoitus, eng. Advanced electronic signature*, *hyväksyttyyn varmenteeseen perustuva kehittynyt sähköinen allekirjoitus, eng. Advanced electronic signature based on a qualified certificate* sekä *kvalifioitu sähköinen allekirjoitus, eng. qualified electronic signature* [14].

2.2.1 Sähköinen allekirjoitus

Sähköinen allekirjoitus on sähköisen tunnistautumisen perusmuoto. Sähköinen allekirjoitus tarkoittaa käytännössä allekirjoitusta, jonka yhteydessä allekirjoittajan ei

tarvitse tunnistautua luotettavasti voidakseen allekirjoittaa. Esimerkiksi kuva käsin tehdystä allekirjoituksesta luetaan tähän tyyppiin kuuluvaksi [14].

2.2.2 Kehittynyt sähköinen allekirjoitus

Kehittynyt sähköinen allekirjoitus on perustason allekirjoitustyypistä korotettu, luotettavampi sähköisen tunnistamisen tyyppi. eIDAS asettaa sille seuraavat vaatimukset [14]:

- Allekirjoituksella on oltava sellainen yhteys allekirjoittajaan, että sen voidaan riittävällä varmuudella olettaa olevan juuri hänen tekemänsä
- Allekirjoittaja on voitava tunnistaa luotettavasti. Allekirjoitus tulee luoda käyttämällä sellaisia sähköisen allekirjoituksen luontitietoja, joiden voidaan luotettavasti olettaa olevan ainoastaan allekirjoittajan hallussa
- Allekirjoitus on linkitettävä allekirjoitettuun dataan niin, että kaikki allekirjoituksen jälkeen tehdyt muutokset voidaan havaita

2.2.3 Hyväksyttyyn varmenteeseen perustuva sähköinen allekirjoitus

Hyväksyttyyn varmenteeseen perustuva sähköinen allekirjoitus on 3. sähköisen tunnistautumisen tyyppi. Siinä allekirjoituksen yhteydessä edellytetään allekirjoittajan henkilöllisyyden todentamista kasvokkain, joko paikan päällä tai etäyhteyden välityksellä [14].

2.2.4 Kvalifioitu sähköinen allekirjoitus

Kvalifioitu sähköinen allekirjoitus on luotettavin eIDAksen tunnistautumisen tyyppi. Siinä vaatimuksena on, että allekirjoitus luodaan siihen tarkoitetulla, hyväksytyllä

allekirjoituksen luontilaitteella. Allekirjoituksen tulee myös perustua hyväksyttyihin elektronisiin sertifikaatteihin. Lain edessä tämän tyypin allekirjoitus on yhtä vahva kuin perinteinen, paperille tehty allekirjoitus [14].

Yhteenveto

Tässä kappaleessa perehdyttiin siihen, mitä tunnistautuminen sekä sähköinen tunnistautuminen käsitteinä tarkoittavat ja mitä Suomen laki säätää niistä. Kappaleessa esiteltiin Suomessa luotu Suomi.fi -palvelu, ja käytiin läpi Euroopan unionin säätämä, sähköistä tunnistautumista säätelevä eIDAS-asetus sekä sen määrittelemät neljä sähköisen tunnistautumisen tasoa.

Vahva sähköinen tunnistautuminen on kriittinen osa nykyaikaista yhteiskuntaa. Se mahdollistaa turvallisen asioinnin esimerkiksi terveyspalveluiden sivuilla tai verkkopankissa. Esimerkiksi monet pankit tarjoavat mahdollisuutta hakea asuntolainaa verkko- tai mobiilipankissa, mikäli henkilö tunnistautuu vahvasti.

Lakien ja säädösten asettamat vaatimukset ovat yksi vahvimmista yhteiskunnan keinoista valvoa tunnistusmenetelmien laatua. Huijauksia ja identiteettivarkauksia voidaan ehkäistä vain laadukkailla menetelmillä. Lait luovat esimerkiksi mobiilivarmenteelle tietyt ehdot, jotka sen on täytettävä voidakseen toimia. Laeilla ja säädöksillä on myös luottamuksen kannalta merkittävä vaikutus tunnistuspalveluille: kun tunnistuspalveluiden tarjoajat ovat lain vaatimissa rekistereissä, käyttäjät luottavat niihin enemmän. Tämä puolestaan parantaa verkossa olevien palveluiden laatua ja monipuolisuutta.

Jotta mobiilivarmenne täyttää sille asetetut ehdot, sen tekniikan tulee perustua monimutkaisiin kryptografisiin menetelmiin, jotka ovat jopa tietokoneille riittävän haastavia murrettaviksi. Laadukkaat menetelmät ehkäisevät merkittävästi myös käyttäjän virheestä aiheutuvia ongelmia. Mobiilivarmenteen tekniseen toteutukseen palataan tarkemmin luvussa 3.

Koska mobiilivarmenteen asema on edelleen kasvamassa vahvassa tunnistautumisessa, turvallisuuden takaaminen on sille erittäin tärkeää. Jotta mobiilivarmenne voi myös tulevaisuudessa toimia, sen tulee lakien ja säädösten täyttämisen lisäksi saavuttaa mahdollisimman laaja käyttäjien luottamus. On erittäin tärkeää, että vahvan tunnistautumisen voi suorittaa muilla tavoin kuin pankkitunnuksilla, sillä kuten aiemmin todettiin, niiden joutuessa rikollisten haltuun, voivat vahingot olla todella suuret.

3 Sähköisen tunnistautumisen protokollat ja tekniikat

Mobiilivarmenne perustuu merkittäviltä osin kryptografiaan. Kryptografia määritellään tekniikkana, jonka avulla viestejä voidaan välittää luotettavasti. Kryptografia tutkii ja kehittää keinoja, joilla lähettäjä voi salata viestejä siten, että vastaanottaja voi purkaa salauksen ja nähdä viestin. Tätä tekniikkaa kutsutaan *päästä päähän salaamiseksi* (eng. end-to-end encryption, E2EE). Usein kryptografiaa käytetään salaamaan viestejä, joiden lähettämiseen käytettävä kanava olisi turvaton ilman kryptografisia menetelmiä [15]. Yleisesti ottaen kryptografiset menetelmät jaetaan kahteen alaluokkaan: *symmetriseen* ja *asymmetriseen salaukseen*. Asymmetrisen salauksen ideana on, että valitaan jokin tietty salausalgoritmi, jota käytetään. Sen jälkeen luodaan tälle algoritmille sopivat, erilaiset mutta matemaattisesti toisiinsa linkitetyt avaimet salauksen luomiseen (yksityinen avain) sekä purkamiseen (julkinen avain). Yksityistä avainta on käytännössä mahdotonta johtaa julkisesta avaimesta, johtuen yksityisen avaimen laskennallisesta monimutkaisuudesta. Vastaanottaja käyttää salauksen purkuun julkista avainta [15] [16]. Symmetrisessä salauksessa lähettäjä ja vastaanottaja joko käyttävät samaa salaista avainta keskenään, tai salaisia avainpareja, joissa kumpikin avain voidaan helposti johtaa toisesta avaimesta [16]. Näitä avaimia ei voida toimittaa osapuolille julkisia kanavia pitkin, vaan ne pitää toimittaa jollakin luotettavalla menetelmällä.

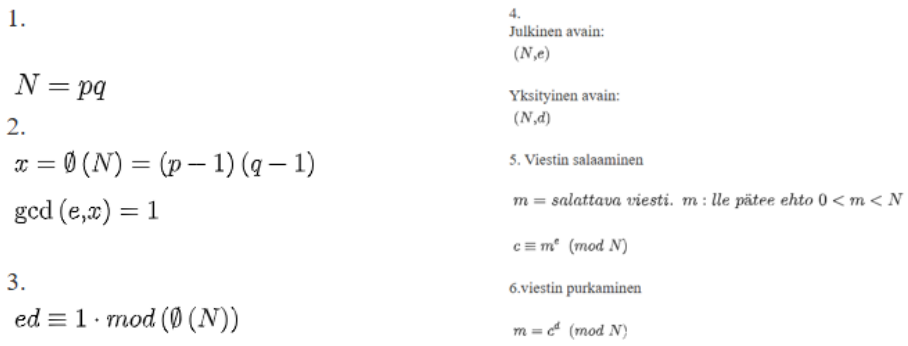
Kryptografian roolia viestien turvallisessa välittämisessä voisi kuvailla seuraavalla esimerkillä: henkilöt Alice ja Bob ovat hyviä ystäviä keskenään. Tällä hetkellä he ovat kuitenkin maantieteellisten sijaintiensa vuoksi tilanteessa, jossa kommunikointi onnistuu vain verkkoyhteyksien välityksellä. Bob haluaisi juuri nyt kertoa Alicelle eräästä isosta salaisuudestaan, eikä hän halua kenenkään muun saavan tietää sitä. Bob on tietoturva-alan asiantuntija, ja hän päättää käyttää viestin välittämiseen Whatsapp-sovellusta. Miksi? Whatsapp on laajalti tunnettu, vahvan suojauksen omaava viestintäsovellus, joka käyttää E2EE -tekniikkaa (end-to-end encryption) viestien salaukseen [17]. Whatsapp ei siis luota pelkkään TLS-salaukseen, joka suojaa vain yhteyden esim. asiakkaan ja palvelimen välillä, vaan viesti pysyy salattuna myös yhteyden ulkopuolella, ja vain oikean avaimen haltija voi purkaa salauksen [17]. Näin Bob saa kerrottua asiansa turvallisin mielin tietoisena siitä, että tekniikan puolesta kukaan muu ei pääse lukemaan hänen viestiään. Seuraavaksi esitellään kolme keskeistä kryptografian alan menetelmää.

3.1 RSA

RSA tunnetaan ensimmäisenä julkisen avaimen infrastruktuurin salausmenetelmänä. Lyhenne tulee algoritmin kehittäjien nimistä; Ronald Rivest, Adi Shamir ja Len Adleman kehittivät menetelmän vuonna 1978.

RSA toimii seuraavasti: Valitaan kaksi isoa päälukua (joilla on sama bittikoko) p ja q, joista lasketaan N = pq (vaihe 1). Seuraavaksi määritetään julkinen eksponentti e, joka on keskenään jaoton Eulerin funktiosta saatavan luvun kanssa (vaihe 2). Jaottomuus tässä tarkoittaa, että näiden kahden luvun ainoa yhteinen tekijä on 1. Sitten lasketaan yksityinen eksponentti d. d:n arvo määräytyy siten, että se kerrottuna e:llä tuottaa tulon, jonka jakaminen luvulla $\phi(N)$ tuottaa jakojäännöksenä luvun 1. $\phi(N)$ tarkoittaa sellaisten lukujen lukumäärää, jotka ovat pienempiä kuin N itse sekä keskenään jaottomia N:n kanssa. Saaduista arvoista muodostetaan julkinen

avainpari (N,e) sekä yksityinen avainpari (N,d) (vaihe 4). Kun viesti m halutaan salata, se korotetaan potenssiin e ja jaetaan sitten N:llä. Saadusta tuloksesta otetaan jakojäännös, joka on salatun viestin arvo kokonaislukuna (vaihe 5). Kun taas salattu viesti, nyt c, halutaan purkaa salaamattomaksi viestiksi m, korotetaan c potenssiin d ja saatu tulos jaetaan N:llä. Saadusta tuloksesta otetaan jakojäännös, joka on salaamattoman viestin arvo kokonaislukuna (vaihe 6) [18]. Kuva 3.1 näyttää RSA:n matemaattisen toteutuksen.



Kuva 3.1: RSA:n matemaattinen teoria

3.2 Elliptisen käyrän salausmenetelmä

Elliptisen käyrän salausmenetelmä (eng. Elliptic Curve Cryptography, ECC) toimii tiivistettynä seuraavasti: ensin valitaan matemaattinen, äärellinen kunta, jonka ylitse valitaan sopiva elliptinen käyrä E. Sitten lasketaan E:n kertaluku, joka on kaikkien E:n pisteiden lukumäärä. Seuraavaksi tarkistetaan, ettei E:llä ole pisteitä, jotka eivät toteuta sen yhtälöä. Etsitään E:ltä tietty piste P, joka tuottaa merkittävän osan E:n muista pisteistä yhteenlaskuoperaation kautta, ja määritetään P:n kertaluku. Tämän jälkeen tulee tarkistaa, ettei nk. MOV-ehto toteudu. MOV-ehto tarkoittaa, että E:n matemaattinen vaikeus ei saa olla muutettavissa tavalliseksi diskreetin logaritmin ongelmaksi, jolloin se voitaisiin murtaa tehokkailla algoritmeilla [18].

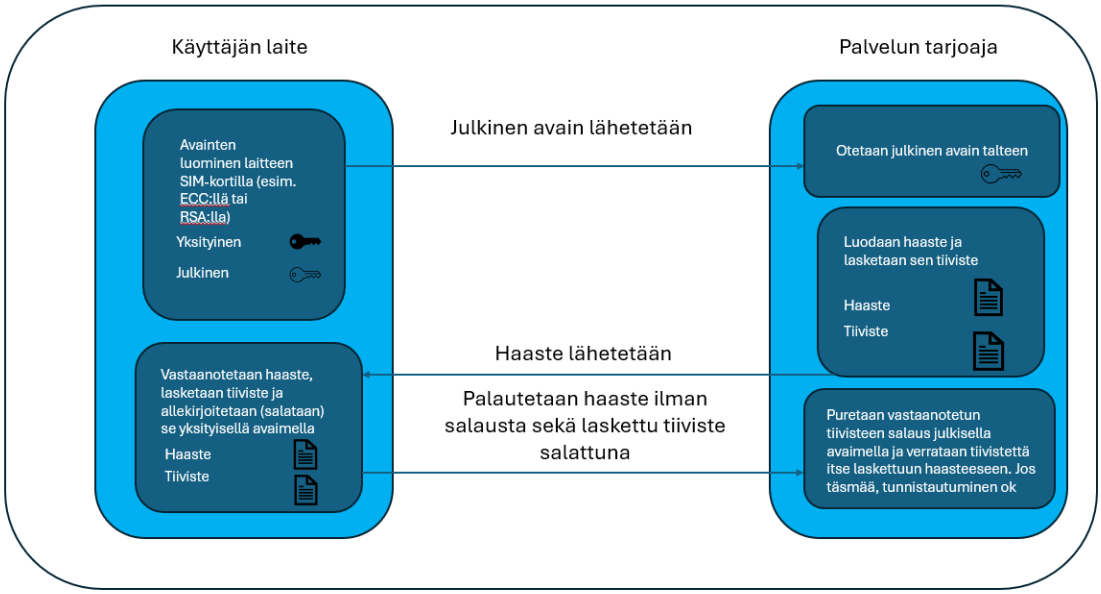
3.3 Julkisen avaimen infrastruktuuri

Yksi mobiilivarmenteen tärkeimmistä mahdollistajista on *julkisen avaimen infrastruktuuri (public key infrastructure, PKI)*. Tässä tekniikassa ideana on luoda avainpareja käyttäen avuksi matematiikan yhtälöitä. Nämä yhtälöt takaavat, että niistä luotuja avaimia voi käyttää vain, jos kumpikin avain on käyttäjällä hallussa. Ainoastaan nämä kaksi nimenomaista avainta toimivat yhdessä. [19]. PKI:n toiminta perustuu avainpareihin, julkiseen ja yksityiseen avaimeen. Avainten luomisessa käytetään esimerkiksi ECC:ä. Myös muita menetelmiä on olemassa, kuten RSA. ECC:n merkittävä etu on siinä, että se tarjoaa esimerkiksi juuri RSA:n kanssa samantasoisen suojauksen paljon lyhyemmillä avaimilla, jolloin se vaatii vähemmän laskentatehoa ja sopii näin myös kevyempiin ympäristöihin. 160-bittinen ECC-avain tarjoaa samantasoisen suojauksen kuin 1024-bittinen RSA-avain [18].

3.4 Mobiilivarmenne

Tunnistusprosessi mobiilivarmenteella etenee siten, että ensiksi käyttäjä valitsee tunnistautumistavaksi mobiilivarmenteen, jonka jälkeen hän syöttää oman puhelinnumeronsa ja lähettää sen tunnistuspalvelun tarjoajalle (jäljempänä "palveluntarjoaja"). Kun tämä on tehty, palveluntarjoaja lähettää käyttäjän SIM-kortille *haasteen*, josta SIM:in tulee laskea tiiviste. Haaste on palveluntarjoajan luoma satunnainen merkkijono, josta lasketaan tiiviste käyttäen matemaattisia tiivistefunktioita, kuten esimerkiksi SHA-256:a, joka tuottaa annetusta haasteesta 256-bittisen tiivisteen [20]. Kun tiiviste on laskettu, kysytään käyttäjältä PIN-koodi. Koodin syöttämisen jälkeen tiiviste allekirjoitetaan PKI:n yksityisellä avaimella. Sitten tiiviste ja haaste lähetetään takaisin palveluntarjoajalle, joka tarkistaa tiivisteen allekirjoituksen omalla julkisella avaimellaan ja vertaa tiivistettä itse laskemaansa tiivisteeseen. Jos tiivisteet täsmäävät, on varmistettu kaksi asiaa: data ei ole korruptoitunut siirret-

täessä sitä laitteelta toiselle, joten yhteyttä ei ole kaapattu, ja käyttäjällä on oikea yksityinen avain, joten hänen voidaan luotettavasti olettaa olevan se taho, joksi hän itseään väittää. Kuva 3.2 havainnollistaa tämän prosessin yksinkertaistettuna. Avaimet luodaan käyttäjän SIM-kortilla hänen ottaessaan mobiilivarmenteen käyttöön. Julkinen avain lähetetään palveluntarjoajalle, kun taas yksityinen avain ei koskaan poistu SIM-kortin niin kutsulta *Secure Element* alueelta.



Kuva 3.2: Mobiilivarmenteen toiminta.

Olennaista on ymmärtää, että PKI ja mobiilivarmenne eivät ole toistensa synonyymeja, vaan mobiilivarmenne on PKI:n päälle rakennettu teknologia, joka hyödyntää avainpareja tunnistaututumiseen. PKI tarkoittaa avainten infrastruktuuria, joka käsittää ratkaisut aina avainten luomisesta niiden tuhoamiseen asti. Käytännössä se siis tarkoittaa kaikkia olemassa olevia menetelmiä avainten luomiseksi, säilyttämiseksi, julkisen avaimen lähettämiseksi, sekä avainparien tuhoamiseksi. Kuva 3.3 havainnollistaa PKI:n ja mobiilivarmenteen suhdetta.

Kuva 3.3: Mobiilivarmenteen ja PKI:n ero.

Yhteenveto

Tässä kappalessa vastattiin TK1:een tutustumalla mobiilivarmenteen taustalla oleviin tekniikoihin, sen toimintaan sekä siihen, kuinka tunnistautuminen mobiilivarmenteella teknisesti tapahtuu. Tutustuttiin kryptografian alaan PKI:n, ECC:n ja RSA:n kautta sekä tarkasteltiin sitä, kuinka kryptografia liittyy mobiilivarmenteen toimintaan.

Mobiilivarmenteen tietoturva ja toiminta perustuvat näille asioille, joten niiden ymmärtäminen on ratkaisevan tärkeää arvioitaessa sen turvallisuutta. Esimerkiksi käyttäjien luotettava autentikointi on mahdollista vain vahvojen kryptografisten me-

netelmien kautta. Tällä hetkellä menetelmät toimivat, mutta tulevaisuudessa tilanne saattaa muuttua. Tähän palataan tarkemmin luvussa 4.

4 Mobiilivarmenteen hyödyt ja uhat

Mobiilivarmenteella on monia hyötyjä, joista merkittävin lienee se, että se vähentää huomattavasti niitä kertoja, jolloin käyttäjän pitää syöttää pankkitunnuksensa. Tällöin ehkäistään merkittävästi sitä riskiä, että tunnukset ja siten myös käyttäjän rahat päätyisivät rikollisten haltuun. Pankkitunnuksilla voidaan tehdä myös muunlaista vahinkoa, kuten esimerkiksi ottaa lainoja käyttäjän nimissä, jos hän ei tajua sulkea tunnuksia tarpeeksi ajoissa. Maailmanlaajuisesti pankkitunnukset olivat kohteena 27,7 prosentissa kaikista kalasteluhyökkäyksistä vuoden 2022 4. neljänneksellä [21]. Mobiilivarmenne ei erikseen tarjoa lisäsuojaa kalastelu-uhkaa vastaan, sillä kalastelu perustuu sellaiselle tekniikalle, jota varten mobiilivarmennetta ei ole suunniteltu.

Yksi mobiilivarmenteen mahdollisista heikkouksista on, että se ei vaadi esimerkiksi näytön lukituksen avaamista, mikäli näyttö on jo valmiiksi auki tunnistuspyynnön saapuessa. Tällöin on mahdollista, että ulkopuolinen voi vahvistuskoodin tietäessään tunnistautua palveluun käyttäjän puhelimella, jos se on esimerkiksi jäänyt hetkellisesti auki toisen ulottuville käyttäjän käydessä esimerkiksi tilan ulkopuolella. Tällöin toinen ihminen voi nähdä arkaluontoisia tietoja, kuten vaikkapa terveystietoja. Tämä voisikin olla yksi kehityksen kohde tulevaisuudessa.

Mobiilivarmenteelle on olemassa muitakin hyökkäystekniikoita kuin kalastelu, joista tutkimuksessa perehdyttiin MITMO -tekniikkaan (man-in-the-mobile). MITMO toimii siten, että siinä käytettävä palvelin sieppaa kahden laitteen välisen kommunikointiyhteyden, katkaisee sen, ja ryhtyy välittämään yhteyttä itsensä kautta.

Päästyään tähän asemaan palvelin voi napata datasta tärkeää tietoa, kuten esimerkiksi puhelinnumeron ja purkaa sen salauksen. Tämän jälkeen palvelin salaa tiedot ja lähettää ne kohdesivustolle. Viimeisenä vaiheena kohdesivusto lähettää istuntoevästeen palvelimelle, joka kaappaa sen itselleen. Tässä on tärkeää huomata, että mobiilivarmenteen kannalta olennainen SIM-kortti ja sillä oleva yksityinen avain eivät missään vaiheessa siirry hyökkääjän haltuun. Hyökkääjä voi kuitenkin kiertää tämän esimerkiksi manipuloimalla käyttäjää hyväksymään hänelle lähetetyn tunnistuspyynnön [22]. Jos manipulointi onnistuu, hyökkääjä pääsee käsiksi uhrin henkilökohtaisiin tietoihin.

Huomattava osa mobiilivarmenteen mahdollisista tietoturvauhkista liittyy vahvasti käyttäjän toimintaan. Näihin uhkiin voidaan lukea esimerkiksi puhelimen näytön vakoilu haittaohjelman kautta sekä peittokuvahyökkäykset, joissa hyökkääjä piirtää haittaohjelman välityksellä saastuneen laitteen ruudulle esimerkiksi väärennetyn tunnistautumissivun, jota käyttäjä sitten klikkaa [23]. Molemmissa tavoissa uhri luovuttaa tietämättään tunnuksensa ulkopuoliselle. Käyttäjä voi ehkäistä kumpaakin näistä uhista myöntämällä sovelluksille vain niiden toiminnan kannalta välttämättömät luvat, lataamalla sovellukset ainoastaan virallisista sovelluskaupoista sekä pitämällä laitteensa päivitettynä [23].

On tärkeää, että vahva tunnistautuminen tehdään mahdollisimman yksinkertaiseksi. Jos tunnistuprosessit sisältävät esimerkiksi monta eri vaihetta, käyttäjät saattavat tehdä tietoturvaa heikentäviä ratkaisuja, kuten esimerkiksi luoda heikkoja salasanoja tai PIN-koodeja.

Kaiken kaikkiaan, kuten yleisestikin tietoturvassa, yhteiskunnan tulee panostaa huijaustapojen tutkimiseen ja niistä raportoimiseen mahdollisimman tehokkaasti. Näin voimme parhaiten varmistaa, että ihmisillä on mahdollisuus pitää itsensä ajan tasalla, sillä tietoturva on ala, joka muuttuu koko ajan. Vastauksena kysymykseen **TK2**: Tällä hetkellä merkittävimmät uhat ja haavoittuvuudet mobiilivarmenteessa

ovat siis se, että näytön lukitusta ei välttämättä tarvitse avata, sekä tietojen kalastelu ja siitä seuraavat, väärät tunnistuspyynnöt. Vielä ollaan kuitenkin tilanteessa, jossa käyttäjä pystyy estämään mobiilivarmenteen murtamisen, koska tunnistukseen tarvittava yksityinen avain pysyy käyttäjän omalla SIM-kortilla. Toistaiseksi mobiilivarmenne kestää siis käyttäjän virheitä hyvin. Käyttäjään voidaan kuitenkin kohdistaa sosiaalista manipulointia, esimerkiksi uhkailua, jotta hän erehtyisi antamaan koodin. Uusia hyökkäystekniikoita kehitetään, joten tekniikan päivittämistä ei saada unohtaa yhteiskunnassa eikä yksilötasolla, vaikka se tällä hetkellä vahva onkin. Tietoturvan kehityksessä ei voida koskaan pysähtyä.

4.1 Tulevaisuuden kehitys

Vaikka mobiilivarmenne tarjoaa tällä hetkellä erittäin vahvaa suojaa teknisiä uhkia vastaan, se saattaa silti kohdata tulevaisuudessa useita merkittäviä uhkakuvia, joihin meidän on vastattava.

Yksi mahdollinen uhka ovat kvanttitietokoneet. Kvanttitietokoneet ovat koneita, joiden toiminta nojaa kvanttimekaniikan periaatteisiin. Merkittävänä erona nykyaikaisiin tietokoneisiin on, että kvanttitietokoneiden perusyksiköitä ovat kubitit [24], kun taas nykyajan tietokoneissa tieto tallennetaan bitteihin. Kubitit ovat huomattavasti tehokkaampia tietojen käsittelyssä niiden superpositioksi kutsutun ominaisuuden ansiosta. Superpositio tarkoittaa sitä, että yhden kubitin arvo voi samanaikaisesti olla sekä 0 että 1, kun taas bitin arvo voi olla yhdellä kertaa vain 0 tai 1 [24].

Nykyaikaisen mobiilivarmenteen perustana olevat ECC ja RSA nojaavat siis siihen, että tietokoneilla menee niiden murtamiseen mielettömän paljon aikaa. On kuitenkin ennustettu, että kvanttietietokoneet ja niihin soveltuvat algoritmit tulevat muuttamaan tilannetta lähivuosikymmeninä. ECC:n ja RSA:n matemaattiset ongelmat saattavatkin yhtäkkiä olla murrettavissa järjellisessä ajassa [25]. Nykyään

on kuitenkin jo olemassa matemaattista teoriaa siitä, miten näitä ongelmia voitaisiin torjua. Tätä paradigmaa kutsutaan *kvanttiturvalliseksi salaukseksi*, (post quantum cryptography, PQC). PQC:ssä keskeisenä ajatuksena on kehittää algoritmeja, jotka ovat matemaattisesti niin haastavia, että ne voitaisiin teoriassa murtaa kvanttilaskennalla, mutta se vie liikaa resursseja. PQC-algoritmit jaetaan 5 ryhmään, jotka esitellään seuraavaksi [25].

4.1.1 Koodipohjainen menetelmä

Tähän ryhmään luetaan kuuluvaksi sellaiset salausmenetelmät, joiden koodi on bittipohjainen ja suorittaa virheenkäsittelyä. Nämä salausmenetelmät ovat saaneet nimensä siitä, että ne pystyvät ratkaisemaan rajallisen määrän virheitä yhdessä bittisekvenssissä [25].

4.1.2 Hajautuspohjainen menetelmä

Hajautuspohjaisessa kryptografiassa ideana on, että kertakäyttöiseen kirjautumiseen käytettäviin instansseihin yhdistetään hajautusfunktiot. Tämän idean esitti alunperin yhdysvaltalainen tietojenkäsittelytieteilijä Ralph C. Merkle. Merkle myös kehitti tähän pohjautuvan tekniikan, jossa suuresta määrästä avaimia lasketaan tiivisteet yksitellen. Saadut tiivisteet yhdistetään puuksi (kryptografinen tietorakenne), jota voidaan käyttää julkisena avaimena. Tämä tunnetaan *Merklen allekirjoitusjärjestelmänä (Merkle Signature Scheme, MSS)* [25].

4.1.3 Isogeniapohjainen menetelmä

Isogeniapohjainen kryptografia perustuu kahden elliptisen käyrän välisen isogenian löytämisen vaikeuteen [25]. Isogenia on kuvaus siitä, kuinka jonkin elliptisen käyrän E pisteitä voidaan kuvata toiselle elliptiselle käyrälle siten, että käyrien ryhmärakenne säilyy. Käytännössä pisteelle luodaan kuvapiste toiselle käyrälle. Ryhmärakenteen

säilymisellä tarkoitetaan puolestaan sitä, että kahdelle pisteelle tehdyn laskutoimituksen tulos on sama riippumatta siitä, suoritetaanko lasku ennen vai jälkeen niiden kuvaamisen [26]. Tämän menetelmän etu on siinä, että tuloksena saadut avaimet ovat kooltaan huomattavasti pienempiä kuin esimerkiksi hila- tai koodipohjaisessa menetelmässä.

4.1.4 Hilapohjainen menetelmä

Hilapohjainen menetelmä perustuu matematiikasta tuttuihin hilarakenteisiin. Tässä hila määritellään käytössä olevien kantavektorien kaikkien mahdollisten painotettujen summien joukoksi. Menetelmän ideana on löytää n-ulotteisesta hilasta lyhyin vektori s. Tässä menetelmässä julkisen avaimen vektori b saadaan laskettua, kun tiedetään julkinen matriisi A, vektori s, sekä laskussa käytettävän häiriön arvo e. Toisin sanoen b = As + e. Tästä nähdään, että vaikka A ja e ovat tiedossa, on yksityisen avaimen (vektori s) laskeminen hyvin haastavaa. Tyypillisesti käytettävä matriisi A on hyvin suuri, joka puolestaan vaatii käytettävältä koneelta huomattavan määrän muistia. [25]

4.1.5 Moneen muuttujaan perustuva menetelmä

Moneen muuttuujaan perustuva menetelmä rakentuu monimuuttujaisten toisen asteen yhtälöiden ratkaisemisen vaikeudelle. Funktio, josta julkinen avain muodostuu, on joukko polynomifunktioita. Tälläinen ongelma on jopa toisen asteen polynomeilla erittäin haastava murtaa. Menetelmän vaikeutta lisää se, että yksityisen avaimen johtaminen julkisesta avaimesta on vielä erikseen tehty vaikeaksi [25].

Yhteenveto

Tässä kappaleessa tarkasteltiin sitä, millaisia hyötyjä mobiilivarmenne tarjoaa käyttäjilleen. Todettiin, että sen tekniikka on vaikea murtaa, ja sen avulla pankkitunnus-

ten käyttöä tunnistautumisessa voidaan vähentää. Kappaleessa tarkasteltiin myös mobiilivarmenteen tekniikkaa vastaan kohdistettuja hyökkäystekniikoita sekä sitä, kuinka käyttäjää voidaan hämätä hyväksymään väärä tunnistustapahtuma. Samalla kuitenkin todettiin, että mobiilivarmenne kestää käyttäjän virheitä hyvin.

Lisäksi pohdittiin, millainen tulevaisuus mobiilivarmenteella on; mitä uhkia esimerkiksi kvanttitietokoneet luovat sille? Minkälaisia keinoja kehittäjillä on suojautua näiltä uhilta? Näitä kysymyksiä varten esiteltiin 5 erilaista kvanttikestävien salausmenetelmien alaluokkaa. Kappaleessa vastattiin **TK2**:een toteamalla, että suurin puute mobiilivarmenteelle lienee tällä hetkellä se, että se ei välttämättä pyydä avamaan näytön lukitusta. Suurimpana uhkana puolestaan nähtiin tietojen kalastelu. Tällä hetkellä varmennetta on erittäin haastavaa murtaa ilman PIN-koodia. Tähän hyökkääjät voivat käyttää sosiaalista manipulointia, ja sitä vastaan tulee taistella jakamalla informaatiota liikkeellä olevista huijaustavoista. Tälläinen käyttäjien informointi on ratkaisevan tärkeää, sillä käyttäjä on mobiilivarmenteen heikoin lenkki, eikä tekniikka auta, jos huijausta ei tunnisteta ja käyttäjä syöttää PIN-koodinsa.

5 Yhteenveto

Tutkielmassa tarkasteltiin mobiilivarmenteen tietoturvaa vahvassa tunnistautumisessa. Alussa perehdyttiin siihen, miksi vahva sähköinen tunnistautuminen ja sitä myöten mobiilivarmenne nykyään ovat tarpeellisia. Kappaleessa 2 perehdyttiin siihen, mitä tunnistautuminen ja sähköinen tunnistautuminen käsitteinä tarkoittavat, miten tunnistautuminen on kehittynyt sekä mitä laissa säädetään niiden vaatimuksista. Kappaleessa 3 perehdyttiin kryptografiaan, sekä siihen miten mobiilivarmenne on teknisesti toteutettu. Lisäksi vastattiin TK1:een. Kappaleessa 4 vastattiin TK2:een, käsiteltiin mobiilivarmenteen mahdollisia uhkia nyt ja tulevaisuudessa sekä sitä, kuinka käyttäjät voivat itse vaikuttaa sen turvallisuuteen. Lisäksi perehdyttiin kvanttilaskennan maailmaan.

Johtopäätöksenä tutkimuksessa todettiin, että mobiilivarmenne on tekniikaltaan hyvin turvallinen. Sen suurimmat uhat liittyvät tällä hetkellä käyttäjän manipulointiin, eivätkä siihen, että tekniikka murrettaisiin. Esimerkiksi yksityinen avain on lähes mahdoton varastaa SIM-kortin *Secure Elementiltä*, eikä varmenteen murtaminen täysin hyökkääjän toimesta onnistu ilman sitä. Mobiilivarmenteen tekniikalla todettiin kuitenkin olevan myös omat heikkoutensa, mutta näiden heikkouksien täydellinen hyödyntäminen edellyttää aina käyttäjän huijaamista. Tärkeintä on siis olla itse tarkkana, asentaa päivitykset ja varmistaa aina, että tietää, minkä tapahtuman tunnistuspyynnön hyväksyy. Huolimatta tämän hetken tilanteesta todettiin myös, että tulevaisuudessa mobiilivarmenteen murtaminen ilman PIN-koodia voi

tulla mahdolliseksi kvanttilaskennan ja -tietokoneiden kehittyessä. Tämä uhka vaikuttaa kuitenkin tällä hetkellä olevan hallussa, perustuen esimerkiksi siihen, että kvanttiturvallisten algoritmien kehitys on edennyt jo merkittävästi. Mobiilivarmenteen tulevaisuus riippuu merkittävästi näiden algoritmien kehityksestä, sillä mikäli ne eivät ole tarpeeksi turvallisia, kvanttitietokoneet voivat tulevaisuudessa murtaa ne.

Lähdeluettelo

[1] A. W. Burks, ”The invention of the universal electronic computer—how the Electronic Computer Revolution began”, *Future generation computer systems*, vol. 18, nro 7, s. 871–892, 2002.

[2] J. Bowen ja R. Wilson, ”Bletchley Park: The Home of Codebreaking: Edited by Robin Wilson”, *The Mathematical intelligencer*, 2026.

[3] N. Packard, ”INTERNET Prehistory: ARPANET Chronology”, *Cogent social sciences*, vol. 9, nro 2, s. 1–47, 2023.

[4] Information Sciences Institute, *RFC 793: Transmission Control Protocol*, University of Southern California, Marina del Rey, CA, U.S.A., 1981.

[5] Information Sciences Institute, *RFC 791: Internet Protocol*, University of Southern California, Marina del Rey, CA, U.S.A., 1981.

[6] B. M. Leiner, V. G. Cerf, D. D. Clark, R. E. Kahn, L. Kleinrock, D. C. Lynch, J. Postel, L. G. Roberts ja S. Wolff, ”A brief history of the internet”, *Special Interest Group On Data Communication Compututer Commununication Review*, vol. 39, nro 5, s. 22–31, 2009.

[7] V. Schafer ja B. G. Thierry, ”The 90s as a turning decade for Internet and the Web”, *Internet histories (2017)*, vol. 2, nro 3-4, s. 225–229, 2018.

[8] T. Berners-Lee, R. Cailliau, J. Groff ja B. Pollermann, ”World-Wide Web: The Information Universe”, *Internet research*, vol. 2, nro 1, s. 52–58, 1992.

[9] S. J. Shackelford ja S. O. Bradner, ”The Web for Free”, teoksessa *Forks in the Digital Road*, New York, NY, U.S.A.: Oxford University Press, 2024.

[10] Kyberturvallisuuskeskus, *Vahva sähköinen tunnistaminen*, https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen, Vierailtu: 2026-01-26.

[11] Suomen valtio, *"Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009"*, 2009.

[12] Digi- ja väestötietovirasto, *Palvelukuvaus - Suomi.fi-tunnistus - Suomi.fi kehittäjille*, https://kehittajille.suomi.fi/palvelut/tunnistus/palvelukuvaus, Vierailtu: 2025-11-06.

[13] T. Mikkola, ”Henkilön vahva sähköinen tunnistaminen”, Opinnäytetyö, Laurea-ammattikorkeakoulu, Suomi, 2009.

[14] D. Gregusova, Z. Halasova ja T. Peracek, ”eIDAS regulation and its impact on national legislation: The case of the Slovak Republic”, *Administrative sciences*, vol. 12, nro 4, s. 1–18, 2022.

[15] A. M. Qadir ja N. Simmons, ”A Review Paper on Cryptography”, teoksessa *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, Barcelos, Portugal, 2019, s. 1–6.

[16] G. J. Simmons, ”Symmetric and Asymmetric Encryption”, *ACM Computing Surveys*, vol. 11, nro 4, s. 305–330, 1979.

[17] S. Ramraj ja G. Usha, ”Signature identification and user activity analysis on WhatsApp Web through network data”, eng, *Microprocessors and microsystems*, vol. 97, s. 104 756–, 2023.

[18] W. J. Caelli, E. P. Dawson ja S. A. Rea, ”PKI, elliptic curve cryptography, and digital signatures”, *Computers & security*, vol. 18, nro 1, s. 47–66, 1999.

[19] V. Lozupone, ”Analyze encryption and public key infrastructure (PKI)”, *International journal of information management*, vol. 38, nro 1, s. 42–44, 2018.

[20] National Institute of Standards and Technology, ”Secure hash standard”, National Institute of Standards and Technology (U.S.), Washington, D.C., tekninen raportti, 2015, NIST FIPS 180–4.

[21] R. Jayaprakash, K. Natarajan, J. A. Daniel, C. V. Chinnappan, J. Giri, H. Qin ja S. Mallik, ”Heuristic machine learning approaches for identifying phishing threats across web and email platforms”, *Frontiers in Artificial Intelligence*, vol. 7, 2024.

[22] Z. Čekerevac, P. Cekerevac, L. Prigoda ja F. Al-Naima, ”Security risks from the modern man-in-the-middle attacks”, *MEST Journal*, vol. 13, nro 1, s. 34–51, 2025.

[23] P. Laka ja W. Mazurczyk, ”User perspective and security of a new mobile authentication method”, *Telecommunication systems*, vol. 69, nro 3, s. 365–379, 2018.

[24] K. S. Balamurugan, A. Sivakami, M. Mathankumar, Yalla Jnan Devi Satya prasad ja I. Ahmad, ”Quantum computing basics, applications and future perspectives”, *Journal of molecular structure*, vol. 1308, s. 137–917, 2024.

[25] A. Shaller, L. Zamir ja M. Nojoumian, ”Roadmap of post-quantum cryptography standardization: Side-channel attacks and countermeasures”, *Information and computation*, vol. 295, s. 105–112, 2023.

[26] J. Hoffstein, J. Pipher ja J. H. Silverman, *An introduction to mathematical cryptography* (Undergraduate texts in mathematics). New York, NY, U.S.A: Springer, 2008.